REANZ TUAKIRI

Rules for participants

October 2019

CONTENTS

1. Introduction

1.1 The purpose of Tuakiri ("the Federation") is to provide a mechanism for connecting members of the education and research sectors including academics, researchers, and students ("End Users") securely and reliably to online information, infrastructure, services and resources.

1.2 Subscription to the Federation is available to organisations and institutions ("Subscribers") which undertake or support education, research or research and development in New Zealand and agree to be bound by these Rules ("Rules").

1.3 The Federation relies on Subscribers, as Identity Providers, correctly and accurately asserting information about the identity of its End Users to other Subscribers who, as Service Providers, will use that information to grant (or deny) access to the services and resources they offer to End Users.

1.4 The scope of the Federation may be extended over time to include a broader range of Subscribers beyond the education and research sectors.

1.5 The electronic exchange of authentication information between End Users, Identity Providers and Service Providers and the provision of support services for Subscribers may be managed by one or more Operators on behalf of the Federation.

2. Authority of this document

2.1 In the event of any conflict or inconsistency between these Rules and any other Tuakiri document these Rules will prevail.

3. Definitions

Term/Abbreviation	*Definition*
AAA	Authentication, Authorisation and Accounting, a term used for describing a technical and legal environment for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services.
Accounting	The tracking of the consumption of resources by users. This information may be used for management, planning, billing, or other purposes. Real-time accounting refers to accounting information that is delivered concurrently with the consumption of the resources. Batch accounting refers to accounting information that is saved until it is delivered at a later time. Typical information that is gathered in accounting may include identity of the End User, the nature of the service delivered, when the service began, and when it ended.
Attribute	Metadata describing either the End User or services provided under the Federation framework. Attributes are used by Service Providers for service provision, including Authentication, Authorisation and Accounting operations. Service Attributes can also be used by End User systems to assist in selecting appropriate Services.
Attribute Release	The release of Attributes for transfer from an Identity Provider to a Service Provider.

Authentication	The process of establishing the digital identity of one entity to another entity. Commonly one entity is a client (an End User, a client computer, etc.) and the other entity is a server (computer). Authentication is accomplished via the presentation of an identity and its corresponding credentials.
Authentication Service	Any activity where an Identity Provider performs the role of End User Authentication and, where relevant, releases the Attributes for its End Users.
Authorisation	The granting of specific types of privileges (including "no privilege") to an entity or an End User, based on their authentication, what privileges they are requesting, the current system state and authorisation rights previously granted by Service Provider to the End User. Authorisation may be based on restrictions, for example time-of-day restrictions, or physical location restrictions, or restrictions against multiple logins by the same user.
Authorisation Service	Any activity where a Service Provider grants access to End Users to services or resources made available by that Service Provider.
Core Attributes	A set of Attributes selected by the Federation that all Identity Providers are required to support.
Credential/s	Is an identifier or set of identifiers (such as a Userid/NetID) being a user name or login ID (NetID) or identifying token (such as a digital certificate) coupled with a "shared secret", usually a password or pass phrase issued by a system to a person that has been mapped authoritatively to an individual. The identity of the person may or

	may not be known to the system when the identifier and the shared secret are issued.
Data	Digital objects including Attributes, Metadata and Logging information.
End User	Any natural person who is a user of resources or services made available under the Federation. An End User must have an association with an Identity Provider registered by the Federation, such that the Identity Provider is authorised by the End User to hold and pass attributes to a Service Provider in order that the End User may gain access to services.
Executive Committee	The governance committee of the Federation, appointed by REANNZ.
Federation	Refers to Tuakiri, the New Zealand access federation, a service offered by REANNZ.
Good Practice	Good practice as generally accepted within the IT industry and determined by the Executive Committee from time to time in the context of the Federation's required standard covering practices for identity management, authentication and authorisation of users of online resources and services.
Identity Provider	Any organisation or institution which has been registered by the Federation as a Subscriber and has a legal relationship with an End User to provide an authentication service for that End User.

Metadata	Structured facts that describe information, or information services as defined by the Federation from time to time.
Participant	A Subscriber that participates in the Federation, including Identity Providers and Service Providers.
Personal Information	Information about an identifiable individual.
REANNZ	At all times refers to Research and Education Advanced Network New Zealand, Ltd.
Rules for Participants	This document updated from time to time defining the Rules for Tuakiri Participants.
Service Provider	Any organisation or institution that is registered by the Federation as a Subscriber and provides access to End Users to services and resources based on a set of Attributes that satisfy their particular authorisation requirements.
Subscriber	Any organisation that subscribes to use the Federation, including Identity Providers and Service Providers.
System	Hardware, software and any other IT asset which when combined are used to process Data.
Tuakiri	Refers to Tuakiri, the New Zealand access federation, a service offered by REANNZ.
Tuakiri Operator	Any entity contracted by the REANNZ to administer day to day operations of the Federation – or REANNZ if no such entity has

	been contracted.
Unique identifier	An Identifier – (a) that is assigned to an individual by a Subscriber ("Entity") for the purposes of the operations of the entity; and (b) that uniquely identifies that individual in relation to that entity; -- but, for the avoidance of doubt, does not include an individual's name used to identify that individual.
Working Day	Any day of the week, other than Saturday, Sunday, Waitangi Day, Good Friday, Easter Monday, Anzac Day or the Sovereign's Birthday, Labour Day and a day in the period commencing with 25 December and ending with 2 January in the following year, the day observed as the anniversary of any province in New Zealand in which an act is to be done and any Public Holiday given in lieu where any of the above days or other designated Public Holidays fall on a weekend.

4. Subscription

4.1 Subscription to the Federation is available to organisations and institutions which undertake or support education, research or research and development in New Zealand, including:

- 4.1.1 Tertiary Education Institutions, such as universities or vocational education institutions;
- 4.1.2 Government, Commercial Research Institutions and not-for-profit entities;
- 4.1.3 Government or Commercial Product and Service Organisations delivering products or services to the education and research sector; and
- 4.1.4 Any other entity approved by the Executive Committee from time to time.

4.2 Subscribers will be registered to use the Federation using an eligibility criteria and registration process determined by the Executive Committee.

5. Fees

5.1 Subscribers shall pay an annual subscription fee to REANNZ.

5.2 The annual subscription fee will be determined by the Executive Committee.

5.3 Failure to pay the annual subscription fee may result in the Subscriber being deregistered by the Federation.

6. Subscriber Responsibilities

6.1 Subscription in the Federation is conditional upon the Subscriber accepting and abiding by these Rules and acknowledging that these Rules are binding upon and enforceable against the Subscriber by REANNZ.

6.2 The Subscriber warrants and undertakes to REANNZ that:

6.2.1 all and any Data, when provided to Tuakiri or another Subscriber (as the case may be), are accurate and up-to-date and any changes to Metadata are provided promptly to the Tuakiri Operator;

6.2.2 it will observe Good Practice in relation to the configuration, operation and security of the System;

6.2.3 it will observe Good Practice in relation to the exchange and processing of any Data and in obtaining and managing the domain name service (DNS) names, digital certificates and private keys used by the System;

6.2.4 it holds and will continue to hold all necessary licences, authorisations and permissions required to meet its obligations under these Rules;

6.2.5 it will not act in any manner which damages or is likely to damage or otherwise adversely affect the reputation of the Federation; and

6.2.6 it will give reasonable assistance to any other Subscriber (including to the Subscriber's identity provider) investigating misuse by an End User.

6.3 Subscribers acknowledge that participation in the Federation does not itself grant them or any of their End Users automatic access to the resources and services of Service Providers, and that such access may be conditional upon each Subscriber or End User agreeing appropriate terms with the relevant Service Provider governing that access. REANNZ will not be responsible for, nor have any liability in respect of, the performance or otherwise of those terms and will not be required to resolve any disputes in relation to those terms.

6.4 The Subscriber acknowledges that the Tuakiri Operator may, without incurring any liability to the Subscriber and without prejudice to any other rights or remedies of the Tuakiri Operator, take such action or may require the Subscriber to take such action, as is necessary in the opinion of the Tuakiri Operator to protect the legitimate interests of other Subscribers or the reputation of Tuakiri or to ensure the efficient operation of the Federation.

6.5 The Subscriber may use the Federation logo in accordance with the Federation logo usage rules as determined and updated from time to time by the REANNZ.

6.6 The Subscriber grants REANNZ the right to:

6.6.1 publish the Subscriber's name and information about services provided for the purpose of promoting Tuakiri and

6.6.2 publish and otherwise use and hold the Subscriber's Metadata for the purpose of administering the operation of the Federation.

7. Tuakiri Responsibilities

7.1 REANNZ, as the Tuakiri Operator, will

7.1.1 provide support services, including a Help Desk service (Tier 1-2), Technical Specialist (Tier 3-4) to Subscribers.

8. Additional Rules for Identity Providers

8.1 A Subscriber which Authenticates an End User via the Federation is acting as an Identity Provider and must comply with the Additional Rules for Identity Providers set out in this Rule 8 and in providing any Attribute warrants to the recipient of that information that it has so complied.

8.2 An Identity Provider may appoint a contractor to undertake some or all of the identity management functions of the Identity Provider. In the event that an Identity Provider appoints a contractor, the Identity Provider must ensure that the contractor complies with these rules as if it were itself an Identity Provider. Each Identity Provider nonetheless will continue to be responsible for the performance of its functions notwithstanding that those functions may have been assigned, sub-contracted or otherwise dealt with.

8.3 Identity Providers must collect or generate the Core Attributes as defined by the Federation (refer Appendix 1).

8.4 Identity Providers may only release Attributes to a Service Provider, or another Identity Provider, with the permission of the End User and must comply with the Rules in section 10.

8.5 Each Identity Provider must have a documented process for issuing credentials that may give access to Service Providers' services or resources. This documentation must be made available to the Federation upon request and the Federation will encourage Identity Providers to make these procedures publicly available.

8.6 Identity Providers must ensure that accurate information is provided about End Users. In particular:

8.6.1 credentials of End Users who are no longer members of the organisation must be revoked promptly, or at least no Attributes must be asserted for such End Users to other Subscribers;

8.6.2 where unique persistent Attributes are associated with an End User, the Identity Provider must ensure that these Attribute values are not re-issued to another

End User for at least 24 months after the last possible use by the previous End User; and

8.6.3 where an End User's status, or any other information described by Attributes, changes, the relevant Attributes must be also changed as soon as possible.

8.7 The Identity Provider must use reasonable endeavours to provide those End Users in respect of whom the Identity Provider provides Attributes with appropriate information on how to use their credentials safely and securely.

8.8 The Identity Provider must ensure that sufficient logging information is retained for the period specified by the Federation to be able to associate a particular End User with a given session that it has authenticated.

8.9 The End User will be responsible for their acts or omissions, including abiding by any licences or other agreements, and complying with the policies set by the Identity Provider and/or the Service Provider. If an End User is subject to conflicting policies, then the more restrictive policy will apply.

8.10 An Identity Provider must provide a mechanism for creation and management of the auEduPersonSharedToken attribute value for an end user.

9. Additional Rules for Service Providers

9.1 A Subscriber who receives the attributes of an End User via the Federation is acting as a Service Provider and must comply with the Additional Rules for Service Providers set out in this Rule 9.

9.2 A Service Provider may appoint a contractor to undertake some or all of the activities required in the supply of the services of the Service Provider. In the event that a Service Provider appoints a contractor, the Service Provider must ensure that the contractor complies with these rules as if it were itself a Service Provider. Each Service Provider nonetheless will continue to be responsible for the performance of its functions notwithstanding that those functions may have been assigned, sub-contracted or otherwise dealt with.

9.3 The Service Provider must comply with the Rules in section 10 and not disclose to third parties including the Federation or any other Subscriber any Attributes supplied by Identity Providers other than those where the relevant End User has given prior informed consent to such disclosure.

9.4 The Service Provider may only use the Attributes for the following purposes:

- 9.4.1 authorising access to the service for which the Attributes have been provided;
- 9.4.2 recording End User access, and retention of records, in order to facilitate traceability of End Users via an Identity Provider;
- 9.4.3 personalisation of a user interface;
- 9.4.4 providing End User support; and
- 9.4.5 generating aggregated anonymised usage statistics for service development and/or for other purposes agreed in writing from time to time with the Identity Provider.

9.5 Attributes may only be used by the service requested by the End User and only for the specified purposes. Service Providers that wish to use attributes in other ways should arrange this either by obtaining positive informed consent from each individual End User,

or by contract with Identity Providers who are then responsible for informing their End Users.

9.6 The Service Provider acknowledges that it is responsible for management of Authorisation to its services and resources and that the Tuakiri Operator and Identity Providers will have no liability in respect thereof.

10. Data Protection and Privacy

10.1 A Subscriber must, when acting in its capacity as a Subscriber of Tuakiri, comply with any applicable legislation in relation to data protection and privacy, including without limitation, the New Zealand Privacy Act 1993. (See New Zealand Privacy Act 1993)

10.2 Without derogating from the general provision of Rule 10.1, a Subscriber must not:

(a) disclose to any other Subscriber any Personal Information except in accordance with Rule 9.3;

(b) assign to any End User a Unique Identifier that to the knowledge of the Subscriber has already been assigned to the End User by any other entity;

10.3 For the avoidance of doubt, the Federation relies on information and the Authentication Service supplied by Subscribers in respect of End Users. The Federation does not provide any Authentication Service, nor does it assign any Unique Identifier to any End User. A Unique Identifier is assigned to an End User by the End User's Identity Provider.

10.4 A Service Provider to which an End User is granted access relies on the Authentication provided by the Identity Provider and the Federation does not assign a Unique Identifier to the End User.

11. Disclaimer and Limitation of Liability

11.1 Unless agreed otherwise in writing between Subscribers, the Subscriber will have no liability to any other Subscriber solely by virtue of the Subscriber's participation in Tuakiri. In particular, participation in the Federation alone does not create any enforceable rights or obligations directly between Subscribers.

11.2 Each Subscriber indemnifies REANNZ as the Tuakiri Operator and shall keep REANNZ indemnified, against any loss suffered, or liability incurred, by Tuakiri as a result of a claim made by an End User for which the Subscriber provided access to the Tuakiri framework to the extent that loss or liability arises as a direct result of the unlawful or negligent act or omission of that Subscriber. The indemnifying Subscriber will not be liable for any special, indirect or consequential loss or damage (including loss of data, loss of income or profit) which would not be recoverable if a claim for damages were made in tort or for breach of contract.

11.3 The Subscriber acknowledges and agrees that REANNZ, as the Tuakiri Operator, has no liability under these Rules or otherwise in respect of:

- 11.3.1 authentication of End Users (which is the responsibility of the relevant Identity Provider);
- 11.3.2 authorisation of End Users (which is the responsibility of the relevant Service Provider);
- 11.3.3 the provision of resources and services by Service Providers;
- 11.3.4 errors or faults in the registration or publication of Metadata; or
- 11.3.5 the fitness of Metadata and Attributes for any purpose save as may be otherwise expressly agreed in writing between REANNZ and the Subscriber.

11.4 The Subscriber acknowledges and agrees that, although the Tuakiri Operator may carry out certain auditing, monitoring and verification activities pursuant to Section 12.1 of these Rules, the Tuakiri Operator will not be obliged to carry out such activities and will have no liability to any Subscriber in respect of such activities.

11.5 Subject to clause 11.6, and to the maximum extent permitted by law, neither REANNZ, nor any other Subscriber will be responsible for any loss or damage of any kind suffered by a Subscriber or an End User arising out of their use of the Tuakiri system or any shared research or education resources or services.

11.6 The Subscriber may, in its absolute discretion, agree variations with any other Subscriber to the exclusions of liability contained in Section 11.5. Such variations will only apply between those Subscribers.

11.7 For the purposes of this Section 11, "Tuakiri" will be deemed to include sub-contractors or agents engaged by REANNZ in relation to the Tuakiri Service.

12. Audit and Compliance

12.1 The Subscriber acknowledges and agrees that the Tuakiri Operator will, on reasonable notice to the Subscriber, have the right to audit the System and the Subscriber's processes and documentation to verify that the Subscriber is complying with these Rules. The Subscriber shall co-operate with and provide such assistance as reasonably required by the Tuakiri Operator in connection with such an audit.

12.2 Whether pursuant to an audit or otherwise, if the Tuakiri Operator has reasonable grounds for believing that the Subscriber is not complying with these Rules including rule 12.1, then the Tuakiri Operator may notify the Subscriber of such non-compliance in sufficient detail to allow the Subscriber to take appropriate remedial action. Following receipt of such notice, the Subscriber must promptly and in any event within 30 days of such notice, remedy the non-compliance. If the Subscriber has not remedied the non-compliance to the Tuakiri Operator's reasonable satisfaction within 30 days of the notice, then the Tuakiri Operator may terminate the Subscriber's participation in the Tuakiri Federation.

13. Termination

13.1 A Subscriber may voluntarily withdraw from the Tuakiri Federation upon 20 Working Days' notice to the Tuakiri Operator.

13.2 REANNZ may discontinue the Tuakiri New Zealand Access Federation service upon no less than 6 Months' notice to all Subscribers, or the end of the subscription period, whichever is the longer.

13.3 The Tuakiri Operator may terminate subscription with immediate effect by giving written notice to the Subscriber, without any compensation or damages due to the Subscriber, but without prejudice to any other rights or remedies which either the Subscriber or the Tuakiri Operator may have, if the Subscriber

13.3.1 has a receiver, voluntary administrator, liquidator, statutory manager or other similar officer appointed over it or over any part of its undertaking or assets; or

13.3.2 passes a resolution for winding up (other than for the purpose of a bona fide scheme of solvent amalgamation or reconstruction) or a court of competent jurisdiction makes an order to that effect; or

13.3.3 enters into any voluntary arrangement with its creditors or ceases or threatens to cease to carry on business; or

13.3.4 is unable to pay its debts or is deemed by an appropriate court to be unable to pay its debts; or

13.3.5 undergoes or is subject to any analogous acts or proceedings under any foreign law, including, but not limited to, bankruptcy proceedings.

14. Consequence of Cessation of Subscription

Following cessation of the Subscriber's participation (under any circumstances):

14.1 The Tuakiri Operator will cease to publish the Subscriber's Metadata and will inform the remaining Subscribers that the Subscriber is no longer a Subscriber;

14.2 the Subscriber will, at its own cost:

14.2.1 cease to hold itself out as being a Subscriber and, if it is an Identity Provider will inform its End Users that its subscription has ceased; and

14.2.2 remove the Federation logo from all of its materials.

15. Changes to Rules

REANNZ may, from time to time, publish amendments to the Rules, which will become binding upon the Subscriber at the time provided for in the amendment. The Tuakiri Operator will make the latest version of these Rules available on the Tuakiri website (www.tuakiri.ac.nz). The Tuakiri Operator will also communicate changes to these Rules in writing to all Subscribers and, where practicable, will provide Subscribers with reasonable advance notice of the amendments to the Rules.

16. Dispute Resolution

16.1 If any dispute arises between the parties arising from or relating to these Rules, REANNZ or the Subscriber will refer the dispute to their respective representatives, whereupon the REANNZ representative and the Subscriber representative will promptly discuss the dispute with a view to its resolution.

16.2 If any dispute cannot be resolved in accordance with Section 16.1 within 10 Working Days, the Subscriber or REANNZ may require that the matter be referred for consultation between the Chief Executive/Vice Chancellor or equivalent of the Subscriber, or their authorised representative, and the Chief Executive of REANNZ. In this event, both the Subscriber and REANNZ will be represented by one or more delegates in consultations which will be held within 15 Working Days of the requirement.

16.3 If a dispute cannot be resolved under Sections 16.1 and 16.2, then the dispute may be referred by either party to the Executive Committee. The Executive Committee may seek expert advice if relevant. The decision of the Executive Committee will be final and binding upon the parties.

17. General

17.1 These Rules are governed by laws of New Zealand which will have exclusive jurisdiction to deal with any dispute which may arise out of or in connection with these Rules.

17.2 If any provision of these Rules is held to be unenforceable by any court of competent jurisdiction, all other provisions will nevertheless continue in full force and effect.

17.3 All notices which are required to be given under these Rules must be in writing and sent, in respect of Tuakiri, to: Research and Education Advanced Network New Zealand, PO Box 3325, Wellington 6140 and, in respect of the Subscriber, to the address of its principal office, or in either case, to any other address in which the recipient may designate by notice given in accordance with the provisions of this Section.

17.4 Except where otherwise stipulated in these Rules, any notice may be delivered by Fast Post or by facsimile transmission. Notice will be deemed to have been served:

17.4.1 if by Fast Post, 48 hours after posting; or

17.4.2 if by facsimile transmission, when dispatched.

17.5 These Rules and all the documents referred to in them supersede all other agreements, arrangements and understandings between the parties in respect of their subject matter, and constitute the entire agreement between them relating to their subject matter.

17.6 The Subscriber may not assign or otherwise transfer its subscription of the Tuakiri Federation without the prior written consent of REANNZ.

18. Copyright & Disclaimer

18.1 This document is copyright to REANNZ 2019. Parts of it, as appropriate, may be freely copied and incorporated unaltered into another document unless produced for commercial gain, subject to the source being appropriately acknowledged and the copyright preserved. The reproduction of logos without permission is expressly forbidden. Permission should be sought from the REANNZ.

18.2 A significant proportion of the material in this document has been adopted or modified from the Australian Access Federation Incorporated and is used with the permission of the copyright owner. The authors are grateful for the support of their Australian colleagues in this endeavour.

18.3 Trademarks: [None specified]

18.4 Internet addresses such as URLs and email addresses listed in this document are for information purposes only. REANNZ does not warrant the accuracy or currency of any information contained in or obtained from a Subscriber's use of these internet addresses. Nor does REANNZ endorse any opinion, view or advice provided by any third party website referenced via hyperlink in these Rules.

18.5 The REANNZ does not accept any responsibility for any loss or damage resulting from the use of the material contained herein.

Appendix 1: Core Attributes

Attribute	Example Values
auEduPersonSharedToken	ZsiAvfxa0BXULgcz7QXknbGtfxk
displayName	Jack Smith
eduPersonAffiliation	faculty
eduPersonEntitlement	urn:mace:auckland.ac.nz:confocalMicroscope http://www.nesi.org.nz/contract/GL123
eduPersonScopedAffiliation	faculty@auckland.ac.nz faculty@cs.auckland.ac.nz staff@auckland.ac.nz student@law.auckland.ac.nz
eduPersonTargettedID	7eak0QQIEhygtPXtpgmu5I5hRnY
eduPersonAssurance	urn:mace:aaf.edu.au:iap:ID:level2
cn	Jack Russell Smith
o	The University of Auckland
mail	j.smith@auckland.ac.nz