Te Puni Kōkiri
MINISTRY OF MĀORI DEVELOPMENT

4 May 2026 File Ref: OIA 50604

[redacted]

Tēnā koe [redacted]

Official Information Act request

Thank you for your information request dated 3 April 2026. You sought the following:

I am making this request under the Official Information Act 1982. The same request is being sent to each of the following agencies:

- *Ministry of Defence*
- *Ministry of Education | Te Tāhuhu o te Mātauranga*
- *Ministry for the Environment | Manatū Mō Te Taiao*
- *Ministry of Foreign Affairs and Trade | Manatū Aorere*
- *Ministry of Health | Manatū Hauora*
- *Ministry of Housing and Urban Development | Te Tūāpō*
- *Ministry of Justice | Tāhu o te Ture*
- *Ministry for Pacific Peoples | Manatū Pasifika*
- *Ministry of Social Development | Te Manatū Whakahiato Ora*
- *Ministry of Transport | Manatū Waka*
- *Ministry for Regulation | Manatū Waeture*
- *Ministry of Māori Development | Te Puni Kōkiri*

I am conducting academic research into New Zealand's reliance on overseas digital infrastructure and AI services, and the implications for New Zealand's sovereignty and decision-making independence. I have made a separate parallel request to MBIE regarding All-of-Government (AoG) procurement arrangements. This request is focused on each agency's own internal arrangements, documents, and policies.

For each agency receiving this request, please provide the following documents:

1. Core Productivity and Email Platform

- *Any contract, licence agreement, or service agreement between your agency and a provider of productivity or email software (e.g. Microsoft 365, Google Workspace, or other), including any schedules specifying term dates*
- *If procured through an AoG arrangement, any agency-level order form, call-off agreement, or accession document relating to that arrangement*
- *Any internal documents specifying data residency or data sovereignty requirements in connection with your productivity platform*

2. Cloud Infrastructure and Storage

- *Any contract, licence agreement, or service agreement between your agency and a cloud infrastructure or storage provider (e.g. Amazon Web Services, Microsoft Azure, Google Cloud), including any schedules specifying term dates*
- *Any security assessment, risk assessment, or privacy impact assessment produced in connection with the use of any cloud infrastructure provider*

- *Any internal documents specifying data residency or data sovereignty requirements in connection with cloud infrastructure*

3. AI Tools and Internal AI Policy

- *Any contract, licence agreement, or service agreement between your agency and a provider of AI tools or services (e.g. Microsoft Copilot, any OpenAI-based product, Google Gemini, or similar), including the provider name, general purpose, and any schedules specifying term dates*
- *Any internal policy, guideline, or usage framework document relating to the use of AI tools by your agency's staff, including any approved or preferred provider lists*
- *Any risk assessment, privacy impact assessment, or security assessment produced in connection with the adoption or use of AI tools at your agency*

Where any document is too large for full release, I would accept a summary, index, or schedule of the relevant documents so that I can make more targeted follow-up requests. I am happy to receive information electronically. I do not require material already publicly available, provided a URL or reference is supplied.

If any part of this request is refused, please advise the grounds for refusal.

Your request has been considered under the Official Information Act 1982 (**Act**).

Six documents have been identified in scope of your request. The documents and my decisions with regard to the release of the information are set out in the table attached as **Appendix A**.

Te Puni Kōkiri uses Microsoft 365 as its core productivity and email platform. This is procured through the All-of-Government (AoG) Microsoft Licensing arrangement administered by the Department of Internal Affairs. The Microsoft Cloud Agreement Memorandum of Understanding (MOU), dated August 2024, sets out the terms between Microsoft Corporation and the Ministry of Māori Development – Te Puni Kōkiri for the provision of Microsoft cloud services, including data handling, privacy, and security obligations.

Regarding cloud infrastructure and storage, Te Puni Kōkiri's primary cloud services are provided through Microsoft Azure as part of the broader Microsoft licensing arrangement. The Microsoft Cloud Agreement MOU encompasses both the productivity platform and cloud infrastructure services.

Te Puni Kōkiri approves use of Microsoft 365 Copilot as an authorised artificial intelligence (AI) tool for a wide range of generative AI use cases and purposes by Ministry kaimahi. The Ministry has internal principles and an appropriate use policy for AI in the workplace.

I trust my response satisfies your request.

You have the right to seek an investigation and review by the Ombudsman of this response. Information about how to make a complaint is available at www.ombudsman.parliament.nz or freephone 0800 802 602.

Please note that Te Puni Kōkiri publishes some of its OIA responses on its website, after the response is sent to the requester. The responses published are those that are considered to have a high level of public interest. We will not publish your name, address or contact details.

If you wish to discuss any aspect of your request with us, including this decision, please feel free to contact us at oia@tpk.govt.nz.

Nāku noa, nā



Manaia King
Hautū, Te Puni Rangatopu | Deputy Secretary, Corporate

Te Puni Kōkiri
MINISTRY OF MĀORI DEVELOPMENT

Appendix A: Documents – OIA request from [redacted] dated 3 April 2026

Item	Date	Document description	Decision
1.	December 2025	Ngā Mātāpono Atamai Hangahanga (AI) Artificial Intelligence (AI) Principles	Released in full.
2.	December 2025	Te Kaupapahere Atamai Hangahanga (AI) Artificial Intelligence (AI) Policy	Released in full.
3.	August 2024	Microsoft Cloud Agreement – Memorandum of Understanding between Department of Internal Affairs and Ministry of Māori Development – Te Puni Kōkiri	Released with some information withheld under section 9(2)(g)(ii).
4.	May 2024	Combined Security Risk and Controls Assessment (Azure Cloud Services and Azure Active Directory)	Released with some information withheld under section (9)(2)(k) and section 9(2)(g)(i).
5.	February 2024	Privacy Impact Assessment, Microsoft Bing Chat Enterprise (Copilot Chat)	Released in full.
6.	February 2019	Privacy Impact Assessment - Microsoft Azure and Office 365	Released in full.

Ngā Mātāpono Atamai Hangahanga (AI)
Artificial Intelligence (AI) Principles

Te Puni Kōkiri
MINISTRY OF MĀORI DEVELOPMENT

Artificial Intelligence (AI) Principles | Ngā Mātāpono Atamai Hangahanga (AI)

These are the guiding principles for our adoption and use of AI tools within Te Puni Kōkiri. They are rooted in ethics, fairness, safety and security and will serve as the guiding framework for all AI policies and procedures that we develop.

In our use of AI, we will:

Protect Māori data sovereignty

We will protect Māori data sovereignty, and the rights of iwi, hapū, whānau and Māori as articulated in Te Tiriti o Waitangi.

Māori data sovereignty refers to the rights of Māori people to control the collection, ownership, and application of their data. There are six key principles:

1. **Rangatiratanga (Authority):** Māori have the right to exercise authority over their data and information.
2. **Whakapapa (Relationships):** Data should be managed in a way that respects the relationships between people, places, and things.
3. **Whanaungatanga (Kinship):** Data governance should foster and maintain Māori kinship ties and community connections.
4. **Manaakitanga (Care and Respect):** Data should be used in ways that enhance the well-being of iwi, hapū, whānau and Māori communities.
5. **Kaitiakitanga (Guardianship):** Iwi, hapū, whānau and Māori have a role as guardians of their data, ensuring it is protected and used responsibly.
6. **Kotahitanga (Unity):** Data practices should promote unity and collective benefit for and with Māori.

These principles ensure that Māori data is managed in a way that aligns with Māori values and aspirations.

Ensure safety and security

We will use AI in ways that ensure the safety and security of our Ministry, our data, information and systems, our kaimahi and stakeholders, and the public.

Be ethical, just and fair

We will use AI in ways that promote fairness, abide by the laws of New Zealand, and do not unjustly harm, exclude, disempower or discriminate against individuals or particular groups.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

In doing so we will:

Be transparent
We will be open about our use of AI and how we use it in our mahi.

Be accountable
We will take responsibility for our use of AI and any decisions we make.

Ensure accuracy and reliability
We will review AI output for accuracy, relevance and potential bias before using it.

Protect privacy
We will keep personal information of kaimahi, stakeholders and the public safe and secure when using AI.

Protect and govern data and information
We will properly manage and control access to our data and information when using AI. We will keep it safe from people viewing or sharing it without permission, whether on purpose or by accident. We will also keep safe any data or information that belongs to others when we use AI.

Commit to ongoing monitoring, learning and development
We will monitor our use of AI and continuously learn to improve. We will stay updated on developments in AI technology, practice, policy and guidelines, and incorporate new tools and practices where appropriate. We will continually learn how to make the best use of AI and incorporate it in our mahi.

Principles approval | Ko te whakaaetanga o te kaupapa

These principles owned and updated by:	It was approved by:	On the date of:	It is due for revision by:
Information Systems	The Deputy Secretary – Corporate	December 2025	December 2027

Acknowledgement [of the use of AI] | Te āhukahuka i [te whakamahinga o te AI]

Artificial Intelligence was used in the development of these principles. Specifically, AI tools were used to:

- Provide ideas and suggestions around potential principles to consider
- Create sentences around specific concepts
- Wordsmith and create a cohesive tone
- Suggest resources

Related documents | Ko ētahi atu kaupapa here

AI Policy for Te Puni Kōkiri
This policy sets out the acceptable use of AI tools within Te Puni Kōkiri.

Information Management Policy
The purpose of this policy is to provide a framework and assign responsibilities for ensuring that full and accurate records are created and managed.

Information Security Policy
This policy defines the principles, expectations, roles, and responsibilities to support Te Puni Kōkiri in upholding its Information Security responsibilities.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Information Security Classification Policy
This policy sets out the rules for protecting and handling information through the use of security classifications.

Personal Information Policy
The purpose of the Personal Information policy is to ensure effective processes are in place for all Personal Information held by Te Puni Kōkiri.

Interim generative AI guidance for the public service. GCDO (July 2023)
This guidance provides initial advice from the data, digital, privacy, procurement, and security System Leaders about Public Service use of generative AI tools. This guidance is intended to support agencies to make more informed decisions about using generative AI, balancing benefits and risks.

Algorithm charter for Aotearoa New Zealand
Algorithm Charter of Aotearoa New Zealand promotes the responsible and ethical use of algorithms in the public sector, ensuring that they are used in ways that are transparent, fair, and accountable. Te Puni Kōkiri is a signatory of this charter.

Te Mana Raraunga Māori Data Sovereignty
This Te Mana Raraunga (TMR) Brief provides a general overview of key Māori Data Sovereignty terms and principles.

Contact | Whakapā mai

If you have any questions regarding this policy, you can contact the Manager, Knowledge Systems.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Te Kaupapahere Atamai Hangahanga (AI)

Artificial Intelligence (AI) Policy

Te Puni Kōkiri
MINISTRY OF MĀORI DEVELOPMENT

Why we have this policy | Ko te pūtake o tēnei kaupapa here

AI technology has grown exponentially in the last few years and is becoming increasingly integrated into our everyday tools. This policy provides guidance that allows us to use AI safely and responsibly at Te Puni Kōkiri. It enables us to take advantage of AI tools to enhance our mahi while also acknowledging and mitigating associated risks such as security and privacy breaches, bias, inaccuracy and lack of Māori data sovereignty.

This policy should be read in conjunction with our AI Principles, the Interim Generative AI guidance for the public service, and the Algorithm Charter for Aotearoa New Zealand.

In cases where issues are unclear, please consult the Manager, Knowledge Systems.

Policy | Kaupapa here

Te Puni Kōkiri provides you with access to approved AI tools to assist you in your mahi. This policy sets out acceptable use of AI in undertaking your mahi.

Use of AI tools | Te whakamahi i ngā taputapu AI

- You must only use AI tools that have been approved by Information Systems and have passed appropriate security and privacy assessments. Contact the Helpdesk for information on how to seek approval for an AI tool or system.
- While using AI tools, you may input information classified as UNCLASSIFIED or IN-CONFIDENCE, provided it complies with all other security and privacy requirements, as defined by Protective Security Requirements.
- While using AI tools, you must not (unless explicitly authorised):
  - input personal data or personal information, or query for personal information about an individual.
  - input any information or data that is classified SENSITIVE or above, as defined by the Protective Security Requirements.
  - input any information that meets the criteria listed under sections 6 or 9 of the Official Information Act 1994.
- You must check the accuracy of all AI output that is incorporated into your mahi and, where possible, cite reference sources.
- You must consider the sovereignty of any Māori data or information being used, either as input or output of AI and, where appropriate, seek permission for use.
- You must not breach intellectual property or copyright belonging to others in your use of AI. When inputting data or information into an AI tool, ensure you have the right to do so.
- You must consider the relevance and potential bias of any AI output that you incorporate into your mahi.
- You must acknowledge the use of AI tools if they have significantly contributed to a piece of mahi or a decision.
- You must take responsibility for any AI outputs you choose to include or incorporate in your mahi.
- You must take responsibility for any decisions you make, even if the decision has been influenced or recommended by AI.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

- You must abide by the Te Tiriti based Māori Data Sovereignty Principles/ Te Rangatiratanga o Rauranga while using AI Tools:
    - Principle 1: Rangatiratanga (Authority) – You must recognise and uphold the right of iwi, hapū whānau and Māori to control their data, ensuring their authority is respected in all data-related activities.
    - Principle 2: Whakapapa (Relationships) – You must commit to manage data in a manner that respects and maintains the connections between people, places, and things, acknowledging the importance of whakapapa.
    - Principle 3: Whanaungatanga (Kinship) – You must take responsibility for the data governance practices to support and strengthen community and family ties, fostering a sense of kinship and belonging.
    - Principle 4: Manaakitanga (Care and Respect) – You must take responsibility to use data in ways that enhances the well-being of iwi, hapu, whānau and Māori communities, demonstrating care and respect in all data practices.
    - Principle 5: Kaitiakitanga (Guardianship) – You must acknowledge your role as a guardian of Māori data, ensuring it is protected and managed responsibly for the benefit of current and future generations.
    - Principle 6: Kotahitanga (Unity) – You must take responsibility that your data practices promote unity and collective benefit, working towards the shared goals and aspirations of iwi, hapū, whānau and Māori communities.

These policy statements ensure that our data practices align with Māori values and principles.

Consequences of breaching this policy | Ngā hua o te whati i tēnei kaupapahere

Any breach of this Policy may constitute misconduct and will be dealt with in accordance with the Disciplinary Process Policy of Te Puni Kōkiri.

Responsibility and enforcement | Ko ngā haepapa me ngā uruhi

This policy applies to all employees and authorised contractors of Te Puni Kōkiri.

Role	Responsibilities
All employees and authorised contractors	Are expected to comply with this Policy.
Deputy Secretary – Governance	The Deputy Secretary – Governance is the Chief Security Officer and is responsible for developing and implementing security procedures consistent with the Protective Security Requirements (PSR) and this policy.
Deputy Secretary – Corporate	The Deputy Secretary – Corporate is the Chief Privacy Officer (CPO) and is responsible for overseeing our information security programme and ensuring compliance with relevant policies and standards, consistent with the PSR.
General Manager – Information Systems	The General Manager – Information Systems is the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) and is responsible for developing and maintaining our information security programme and ensuring compliance with relevant policies and standards, consistent with the PSR.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Managers	Managers are responsible for ensuring their employees complete all relevant training and adhere to the policy.

Monitoring and revision [of the policy] | Te aroturukitanga me te whakahounga [o te kaupapahere]

Classification thresholds and privacy guidelines for AI input will be reviewed regularly to ensure they align with PSR requirements and the organisation's risk appetite.

Policy approval | Ko te whakaaetanga o te kaupapa

This policy is owned and updated by:	It was approved by:	On the date of:	It is due for revision by:
Information Systems	The Deputy Secretary – Corporate	December 2025	December 2027

Acknowledgement [of the use of AI] | Te āhukahuka i [te whakamahinga o te AI]

Artificial Intelligence was used in the development of this policy. Specifically, AI tools were used to:

- Create sentences around specific concepts
- Wordsmith and create a cohesive tone
- Suggest resources

Related documents | Ko ētahi atu kaupapa here

AI Principles for Te Puni Kōkiri
These principles set the guiding framework for any policies and processes developed within Te Puni Kōkiri for use of AI tools.

Information Management Policy
The purpose of this policy is to provide a framework and assign responsibilities for ensuring that full and accurate records are created and managed.

Information Security Policy
This policy defines the principles, expectations, roles, and responsibilities to support Te Puni Kōkiri in upholding its Information Security responsibilities.

Information Security Classification Policy
This policy sets out the rules for protecting and handling information through the use of security classifications.

Personal Information Policy
The purpose of the Personal Information policy is to ensure effective processes are in place for all Personal Information held by Te Puni Kōkiri.

Interim generative AI guidance for the public service. GCDO (July 2023)
This guidance provides initial advice from the data, digital, privacy, procurement, and security System Leaders about Public Service use of generative AI tools. This guidance is intended to support agencies to make more informed decisions about using generative AI, balancing benefits and risks.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Algorithm charter for Aotearoa New Zealand
The Algorithm Charter for Aotearoa New Zealand promotes the responsible and ethical use of algorithms in the public sector, ensuring that they are used in ways that are transparent, fair, and accountable. Te Puni Kōkiri is a signatory of this charter.

AI Principles and Māori Data Sovereignty
Tiriti-based AI Principles of Tino rangatiratanga, Equity, Active protection, Mana whakahaere, Mana motuhake, Tapu/noa.

Te Mana Raraunga Māori Data Sovereignty
This Te Mana Raraunga (TMR) Brief provides a general overview of key Māori Data Sovereignty terms and principles.

Glossary of terms | Te rārangi kupu

AI (Artificial intelligence)

Artificial intelligence (AI) is a field of computer science and machine learning that allows computer systems to perform tasks that typically require human intelligence. These tasks can include things like learning from data, recognizing patterns, making decisions and solving problems. AI enables computers to think, learn, and act in ways that mimic human intelligence, allowing them to tackle complex tasks and adapt to new situations without explicit programming.

GenAI (Generative AI)

Generative AI (GenAI) is a type of AI that uses prompts to generate responses that closely resemble human-created content. This content can be in the form of text, images, video, or audio.

Input

Input refers to any text, image, audio, video, code, link, data, dataset, or document provided as a prompt to an AI tool.

Māori Data

Is defined as the “Digital or digitisable information or knowledge that is about or from Māori people, language, culture, resources, or environments”. Māori Data is a Taonga and subject to Māori Governance.

Māori Data Sovereignty

Is “Māori Data Governance. The principles, structures, accountability mechanisms, legal instruments, and policies through which Māori exercise control over Māori data”.

Māori Data Sovereignty Principles/ Te Rangatiratanga o Rauranga

Is a modified set based on the academic position of Te Mana Raraunga to embed more traditional tikanga and Te ao Māori perspectives and individual, whānau, hapū, marae, rōpū and Iwi Sovereignty is recognised as outlined in Te Tiriti o Waitangi.

Output

Output in Generative AI refers to any text, image, audio, video, code, or document generated by an AI tool.

Contact | Whakapā mai

If you have any questions regarding this policy, you can contact the Manager, Knowledge Systems.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Te Tari Taiwhenua
Internal Affairs

Memorandum

in connection with the Microsoft Cloud, Software and Services Agreement with Microsoft Ireland Operations Limited

The Parties

The Sovereign in Right of New Zealand acting by and through the Chief Executive of the Department of Internal Affairs **(Lead Agency)**

and

Ministry of Māori Development -Te Puni Kokiri **(Affiliate)**

The Memorandum

The documents forming the Memorandum of Understanding are

1. This Memorandum, including the Terms Specific to the Framework Agreement.
2. All other Memoranda executed by the parties in relation to any other Framework Agreements.
3. The Memorandum of Understanding – Standard Terms.

How to read the Memorandum of Understanding

1. Together the above documents form the whole Memorandum of Understanding.
2. Defined terms are either defined in this Memorandum or in the definitions section in the Memorandum of Understanding – Standard Terms.

Acceptance

In signing this Memorandum each party acknowledges that it has read and agrees to be bound by it.

For and on behalf of the **Lead Agency**:

K. McCashin

(signature)

Name: Kevin McCashin

Position: Manager, ICT Capabilities and Change

Date: 23/08/2024

For and on behalf of the **Affiliate**:

(signature)

Name: Manaia Paki King

Position: Deputy Secretary, Corporate

Date: 23/08/2024

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Terms specific to the Framework Agreement

1. Purpose

1.1 Framework Agreement

The Lead Agency has entered into the Microsoft Cloud, Software and Services Agreement with Microsoft Ireland Operations Limited (**Vendor**) dated on or about August 2024 (the **Framework Agreement**).

1.2 Affiliate Agreement

Eligible Agencies can purchase Services under the Framework Agreement following execution of this Memorandum with the Lead Agency and execution of an Affiliate Agreement with the Vendor.

1.3 Purpose of Memorandum

The Lead Agency administers the Framework Agreement. This Memorandum sets out the Lead Agency's and Affiliate's rights and obligations, as between each other, and other matters related to the Lead Agency's role in managing the Vendor and the Framework Agreement.

1.4 MOU and standard terms

The Memorandum of Understanding – Standard Terms sets out the standard terms that apply to the MOU, and this Memorandum sets out the particular terms that are required for the Framework Agreement.

1.5 Affiliates responsible for use of Services

The Services are the Vendor's standard offerings. No Services have been assessed by the Lead Agency for any particular use and no open advertisement procurement process has been conducted. Affiliates remain responsible for ensuring their own use of the Services are appropriate and that any procurement process obligations are met.

2. Governance Contact details

2.1 Lead Relationship Manager

The name and contact details for the Lead Agency's Lead Relationship Manager (see clause 3.1(a) of the Memorandum of Understanding – Standard Terms) are as follows:

Roger Bowron
Supplier Portfolio and Contracts Manager
Digital Public Service Branch
AoG Services Delivery
Department of Internal Affairs
45 Pipitea Street
PO Box 10-526
Wellington 6143
Email: subscriptions@dia.govt.nz

RELEASED UNDER THE OFFICIAL INFORMATION ACT

2.2 Affiliate Representative

The name and contact details for the Affiliate Representative (see clause 3.1(b) of the Memorandum of Understanding – Standard Terms) are as follows:

Stuart Gregory
General Manager, Information Systems
Te Puni Kōkiri House, 143 Lambton Quay, Wellington 6011
9(2)(g)(ii) [redacted]

2.3 Contact Details for Notices

The parties' contact details for notices (see clause 13.2 of the Memorandum of Understanding – Standard Terms) are as follows:

Lead Agency

Manager Commercial & Supplier Relationships
Digital Public Service Branch
Department of Internal Affairs
45 Pipitea Street
PO Box 10-526
Wellington 6143
Email: subscriptions@dia.govt.nz

The Affiliate

Stuart Gregory
General Manager, Information Systems
Te Puni Kōkiri
Te Puni Kōkiri House, 143 Lambton Quay, Wellington 6011Address
9(2)(g)(ii) [redacted]

Copied to:
Chief Legal Advisor
Department of Internal Affairs
Level 6
42 Pipitea Street
Wellington 6140
Email: legalnotices@dia.govt.nz

3. Additional terms for Microsoft Cloud, Software and Services Agreement

3.1 Definitions

The definition of Eligible Agency in the Memorandum of Understanding – Standard Terms shall not apply to this MOU in respect of the Microsoft Cloud, Software and Services Agreement and instead the following definition shall apply:

Eligible Agency has the meaning set out below. If the Lead Agency and Microsoft agree to amend the Microsoft Cloud, Software and Services Agreement by amending the definition of "Eligible Agency" in such agreement, the amended definition will also apply to this MOU:

(a) each department as defined in section 5 of the Public Service Act 2020;

(b) the New Zealand Defence Force, the New Zealand Police, the Parliamentary Counsel Office, Office of the Clerk of the House of Representative, the Parliamentary Service; Parliamentary Corporation, and Parliamentary Services Commission;

RELEASED UNDER THE OFFICIAL INFORMATION ACT

(c) each Crown entity, as defined in section 7 of the Crown Entities Act 2004;

(d) each organization listed in schedules 4, 4A and 6 to the Public Finance Act 1989;

(e) the Reserve Bank of New Zealand;

(f) the Office of the Controller and Auditor-General, the Office of the Ombudsmen, and the Office of the Parliamentary Commissioner for the Environment;

(g) the following State Owned Enterprises as listed in the first schedule to the State-Owned Enterprises Act 1986:

1) Airways Corporation of New Zealand Limited;

2) Animal Control Products Limited;

3) Electricity Corporation of New Zealand Limited;

4) Transpower New Zealand Limited;

(h) the Local Government Commission, and any local authority or any council-controlled organisation (both as defined in the Local Government Act 2002);

(i) Teaching Council of Aotearoa New Zealand; and

(j) any agency that is not an entity referred to in paragraphs (a) to (i) above, but that is located in New Zealand and the Lead Agency and Microsoft agree in writing is eligible or is an "eligible entity" as defined in the Microsoft Government Eligibility Definition document applicable to New Zealand, which is published by Microsoft from time to time at http://www.microsoftvolumelicensing.com or at a successor site that Microsoft identifies. For the avoidance of doubt, any minimum or required number of license orders (or similar) specified in that Government Eligibility Definition document shall not apply for the purpose of determining whether an agency is an "eligible entity" under that document.

An agency is not an Eligible Agency where the agency:

(k) is a State enterprise as defined in section 2 of the State-Owned Enterprises Act 1986 or a publicly listed company (or a subsidiary of either of those types of entities), unless that State enterprise or company is listed in (g) above or agreed in writing by the Lead Agency and Microsoft to be eligible in accordance with section (j) above;

(l) is a "Qualified Educational User" that qualifies for Microsoft's academic edition products, as defined in the New Zealand specific document athttps://www.microsoft.com/licensing/docs/view/Industries--Education?lang=1 (or a successor site);

(m) is a "Private School" or a "State School" as defined in the Microsoft School Framework Agreement for the New Zealand Ministry of Education (Framework Agreement number N37) between the Crown and Microsoft Operations Pte. Limited (or any successor agreement); or

(n) has breached any license agreement with any Microsoft affiliate and subsequently had that license agreement terminated by that Microsoft affiliate in accordance with its terms.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

3.2 Other terms

(a) **Information sharing**: The Microsoft Cloud, Software and Services Agreement includes an information sharing regime as Schedule 3 to the Microsoft Cloud, Software and Services Agreement, which is incorporated into and forms part of all Affiliate Agreements. Schedule 3 to the Microsoft Cloud, Software and Services Agreement is attached as Appendix A to this Memorandum. The Affiliate consents to the sharing of information as set out in Appendix A.

(b) **Security breaches and outages**: If the Affiliate becomes aware that a significant security breach or significant system outage has occurred in respect of the Microsoft products or services that it purchases under the Microsoft Cloud, Software and Services Agreement, the Affiliate will use reasonable endeavours to promptly notify the Lead Agency and provide the Lead Agency with reasonable information in relation to the security breach or outage. The Lead Agency may share this information with the National Cyber Security Centre. Significant security breaches or significant system outages should be notified to ICTCCOpSec@dia.govt.nz

(c) **Administration Fee**: In addition to clause 9 of the Memorandum of Understanding – Standard Terms, the following provisions apply in respect of the Administration Fee:

(i) Amount

(1) As at the Commencement Date, the Administration Fee is 1.75% of the fees paid by the Affiliate under the Affiliate Agreement.

(2) The Lead Agency may request reports from the Affiliate, the Affiliate's reseller (if any) or the Vendor to enable the Lead Agency to confirm the fees paid by the Affiliate under the Affiliate Agreement.

(ii) GST

The Affiliate will also pay to the Lead Agency the amount of any goods and services tax (GST) that is chargeable on the Administration Fee.

(iii) Invoices

The Lead Agency will invoice the Affiliate for the Administration Fee annually, or in accordance with any other period as agreed in writing by the parties, in arrears for the fees paid by the Affiliate under the Affiliate Agreement within the period to which the invoice relates. The payment period covered will be listed on each invoice.

(iv) Payment

The Affiliate will pay to the Lead Agency the amounts specified in each invoice by the 20th of the month following the month in which the invoice is received by the Affiliate.

(v) Invoice disputes

The Affiliate shall promptly notify the Lead Agency in writing if it disputes any invoice or any amount in an invoice. The Affiliate:

(1) may withhold payment of any reasonably disputed sum until the dispute is resolved;

(2) shall pay to the Lead Agency the undisputed amount of the invoice in accordance with clause (iv) above; and

RELEASED UNDER THE OFFICIAL INFORMATION ACT

(3) shall deal with the disputed amount of an invoice, or a disputed invoice, in accordance with clause 8 of the Memorandum of Understanding – Standard Terms.

(vi) Purchase order, billing information and other requirements

The Lead Agency will include any specific information the Affiliate requires on its invoices, as set out below:

(1) Affiliate Purchase Order Number (if applicable):

[insert details].

(2) Affiliate Billing Name (if applicable and different from Affiliate Representative):

[insert details].

(3) Any further information:

[insert details].

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Appendix A

SCHEDULE 3: INFORMATION SHARING

1. INTRODUCTION AND OBJECTIVE

1.1 **Introduction**: This Schedule 3 (Information Sharing) outlines the information that Microsoft may provide to the Department and the National Cyber Security Centre (**NCSC**), and the information that the Department, the NCSC and Enrolled Affiliates can share with each other, in relation to the Master Agreement and Affiliate Agreements.

1.2 **Notification**: The Department will notify Eligible Agencies of this Schedule 3 and that this Schedule 3 forms part of their Affiliate Agreements.

1.3 **Interpretation**: Unless the context otherwise requires, terms defined in the Agreement bear the same meaning in this Schedule.

2. RELEASE OF INFORMATION

2.1 **Confidential Information**

This Schedule 3 is subject to clause 6 of the Master Agreement (concerning Confidential Information). The parties each agree that:

(a) they will not release the other party's Confidential Information other than under this Schedule 3 or in accordance with the Master Agreement; and

(b) this Schedule 3 is not intended to change the character or quality of Confidential Information.

2.2 **Enrolled Affiliates**

Microsoft will notify the Department when an Eligible Agency becomes an Enrolled Affiliate.

2.3 **Information sharing**

Each party agrees that the other parties may share information:

(a) identified in Appendix A (Information Sharing Table);

(b) with the parties identified in Appendix A as those to whom the information can be shared, and their legal counsel,

provided that:

(c) where there is an agreement identified in Appendix A for a party, that agreement is executed by the relevant parties before the information is shared and such parties are required to protect Confidential Information on terms no less protective than Section 6

RELEASED UNDER THE OFFICIAL INFORMATION ACT

(Confidentiality) of the Master Agreement;

(d) in the case of sharing information with NCSC in accordance with this section, NCSC is required via a Memorandum of Understanding between the Department and the Government Communications Security Bureau to protect Confidential Information on terms no less protective than Section 6 (Confidentiality) of the Master Agreement;

(e) only the Department or Microsoft are permitted to share the "Agreement documents" with any other party. Where the Department shares “Agreement documents” as defined in Appendix A, these must be provided in a read-only format; and

(f) unless otherwise specified in this Schedule, the NCSC must only request access to information it is eligible for as specified in Appendix A directly from the Department, and not from Microsoft, except where the NSCS is requesting such information as an Enrolled Affiliate.

2.4 **Consumption reporting**

Microsoft will provide consumption reporting to the Department as set out in Schedule 4 (Governance) to assist the Department to understand and monitor the use of Products and Professional Services by Enrolled Affiliates and to enable the Department and the NCSC to perform their roles as functional and system leaders in the context of the New Zealand government (“Purpose”). Such reporting is made available by Microsoft:

(a) 'as-is' without any warranty, whether express or implied by statute;

(b) shall be deemed Microsoft Confidential Information and, subject to this Schedule, shall be treated as such in accordance with Section 6 (Confidentiality) of the Master Agreement; and

(c) shall be provided directly to the Department only. NCSC may acquire the relevant consumption reporting by request to the Department.

The Department agrees that the consumption reporting:

(d) will only be used for the Purpose provided and solely for the Department’s and NCSC's internal purposes; and

(e) notwithstanding Section 6 (Confidentiality) of the Master Agreement, the consumption reporting and the information within such reports shall not, unless Microsoft provides its prior written agreement, be reproduced, modified or provided to any third party, except as required by Section 6(c)(iv) of the Master Agreement, including to:

(i) Eligible Agencies even as part of any meetings that are conducted in accordance with Schedule 4 (Governance) where an Eligible Agency is in attendance;

(ii) any Representatives of the Department except for employees of the Department or the Department’s legal counsel and only in accordance with Section 6 (Confidentiality) of the Master Agreement; and

RELEASED UNDER THE OFFICIAL INFORMATION ACT

(iii) any Representatives of the NCSC except for employees of NCSC or NCSC's legal counsel and only in accordance with Section 6 (Confidentiality) of the Master Agreement.

Microsoft reserves the right to suspend the provision of consumption reporting pending an investigation into the Department and/or NCSC's compliance with this paragraph 2.4 and will continue to withhold it thereafter if Microsoft reasonably finds that the Department or NCSC has not complied. For the purposes of this paragraph, "consumption" means Products purchased and used by Eligible Agencies through an Enrollment.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Appendix A: Information Sharing Table

Parties with whom information may be shared	Information that can be shared							
	Agreement documents	**Amendments**	**Consumption information**	**Projects involving artificial intelligence**	**Projects involving indigenous data**	**Major Incidents**	**Security Incidents**	**Operational Performance**
	All template documents that, once executed, form an Affiliate Agreement, including the Master Agreement and its Schedules	Summary Register of contract amendments entered into between Microsoft and Enrolled Affiliates to include details of amendment including discounts.	Information regarding an Enrolled Affiliate's use of Products and Professional Services, including fees paid, number of licenses purchased and amounts of Online Services consumed	Information regarding how Enrolled Affiliates have implemented AI in significant projects	Information regarding how indigenous data (including Māori data) was treated, including classification and security controls	Information regarding major service outages affecting multiple Eligible Agencies, including root cause analysis (if known), agencies impacted, impact to agencies (to the extent known by Microsoft), post incident reports	All information regarding Security Incidents shared by Microsoft with an Enrolled Affiliate in accordance with the Data Protection Addendum	All SLA reports provided to the Department by Microsoft

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Department **Master Agreement**	√	√	√	√	√	√	√	√
Microsoft **Master/Affiliate Agreement**	√	√	√	√	√	√	√	√
Enrolled Affiliates **Affiliate Agreement**	√ (excluding Governance schedule)	X	X	√	√	√	√	√
Eligible Agencies **MOU with confidentiality obligations similar to section 6 of the Agreement**	√ (excluding Governance schedule)	X	X	X	√	X	X	X
NCSC **MOU**	√	√	√	√	√	√	√	√

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Te Puni Kōkiri
MINISTRY OF MĀORI DEVELOPMENT

Te Kāwanatanga o Aotearoa

Document 4

Kaupapa: Azure Cloud Services and Azure Active Directory

Security Risk and Controls Assessment

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Summary

This report documents the findings of the Information Security Risk Assessment and Controls Validation Audit carried out for the use and operation of Azure Clound Services and Azure Active Directory

Whakatauki

Tē tōia, tē haumatia
Not dragged, not shouted

The metaphor is based on the traditional method of launching a large canoe. The dragging of the canoe cannot be done without its being followed by the shouting. Nothing can be achieved without a plan, a workforce and a way of doing things.

Creative Commons

This work is licensed under the Creative Commons Attribution 4.0 New Zealand License.

To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/4.0/

Published by

Te Puni Kōkiri
ISBN: 978-0-478-34561-2
Whiringa-ā-nuku/October 2015

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Document Control

General Information

Document Title	2024 05 01 IS Combined SRA and CVA Azure
Author	Phillippa Bedford

Revision History

Version	Date	Author	Description
0.1	01/05/2024	Phillippa Bedford	Initial Draft

Distribution List

Name	Organisation	Title
Stuart Gregory	Te Puni Kōkiri	Director, Technology and Systems
Arahia Wade	Te Puni Kōkiri	Manager, Risk and Assurance

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Contents

General Information 2
Revision History 2
Distribution List 2

Section 1. Executive Summary 4
Section 2. Key Points 5
2.1 Risks and Controls 5
2.2 Recommendations 6

Section 3. Risk Acceptance 7
Section 4. Context 8
4.1 Solution Overview 8
4.2 Business Impact 8
4.2.1 Information Classification 8
4.2.2 Confidentiality 8
4.2.3 Integrity 8
4.2.4 Availability 8
4.2.5 Privacy 8

Section 5. Review Details 9
5.1 Introduction 9
5.2 Approach 9
5.3 Scope 9

Section 6. Current Risk Matrix 10
Section 7. Target Risk Matrix 11
Section 8. Detailed Risk Findings 12
Section 9. Controls Validation 15
Appendix 28

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Section 1. Executive Summary

This report documents the finding of the Information Security Risk Assessment and Controls Validation Audit carried out for the use and operation of Microsoft Azure Cloud and Azure Active Directory (Azure) at Te Puni Kōkiri.

Microsoft offers subscription-based services that allow customers to build or move their physical infrastructure to a virtual environment (into the cloud). Azure provides virtualised compute, storage and network services that can be upgraded and maintained without physical hardware. Azure Active Directory is a cloud-based identity and access management service. This service allows users to access other resources such as Microsoft 365, the Azure Portal and other applications. Azure Active Directory can also be utilised to access other internal resources such as the Te Puni Kōkiri Intranet, along with any other cloud applications.

Azure has been issued a Service Security Certificate (SSC) by the Department of Internal Affairs (DIA) in its capacity as Government Chief Digital Officer (GCDO). The SSC has been issued on 31 August 2022 and is valid until 30 June 2025. The SSC provides agencies with a baseline security assurance for the use of the standard Azure services in the absence of specific agency context or system architecture. Agencies are required to confirm their own controls are in place. That is the function and purpose of this Risk Assessment.

The Risk Assessment follows the Te Puni Kōkiri Certification and Accreditation process, undertaken in line with the New Zealand Information Security Manual (NZISM) standards.

Four (4) risks have been identified as being applicable to the use of Azure by Te Puni Kōkiri. Risks have been rated based on the impact to Te Puni Kōkiri if the risk eventuated, and the likelihood of the risk occurring. (Impact and Likelihood ratings tables can be found in Section 10: Appendix)

R01: Inadequate Protection of Data in Transit and at Rest s9(2)(k)
R02: Unauthorised Access to Systems s9(2)(k)
R03: Misconfiguration of Azure s9(2)(k)
R04: Data Sovereignty and Jurisdictional Risk (s9(2)(k)

The risk assessment of Te Puni Kōkiri's consumption of Azure identified 19 controls that should be implemented to reduce the likelihood and / or the impact to Te Puni Kōkiri if the risk is realised. These controls are documented in the Te Puni Kōkiri Controls Catalogue. These controls are recommended to reduce the risk levels from the current risk rating to the target risk rating.

On completion of controls validation, the Current Risk levels to Te Puni Kōkiri were calculated, with the result that two (2) risks were assessed as **High,** one risk was assessed as **Medium,** and one (1) risk assessed as **Low.** No risks were identified as **Extreme.**

The current overall risk level for the use for Azure at Te Puni Kōkiri is **Medium.**

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Section 2. Key Points

This section summarises and comments on the current and target risk matrixes, and the detailed risk findings and controls from the controls catalogue.

2.1 Risks and Controls

Risk Summary Table: Summary of the total number of risks at each level. Current Risks indicate what the risk environment is like with only the current assessed controls in place, while Target Risks indicate the risk environment with all controls properly applied.

Risk Type	Very High	High	Medium	Low
Current Risks	-	2	1	1
Target Risks	-	1	2	1

Control Summary Table: Summary of control status and implementation. For detailed control descriptions see the Controls Catalogue.

Control ID	Control Title	Status	Related Risks
C101	Role Based Access Control	**Effective**	R02, R03
C103	Multi-Factor Authentication	**Effective**	R02
C104	Management of Privileged Access	**Effective**	R02, R03
C105	Information Transfer	**Effective**	R04
C107	Password Policy	**Partially Effective**	R02
C203	Business Continuity	**Partially Effective**	R04
C401	Data Encryption in Transit	**Effective**	R01
C402	Data Encryption at Rest	**Effective**	R01
C406	Security Information and Event Management (SIEM)	**Effective**	R01, R02
C407	Event Logging, Monitoring and Auditing	**Effective**	R01, R02
C408	Intrusion Detection and Prevention	**Effective**	R01
C502	Documentation	**Partially Effective**	R03
C503	Cryptographic Key Management	**Effective**	R01
C511	Contracts and Service Level Agreements	**Effective**	R04

RELEASED UNDER THE OFFICIAL INFORMATION ACT

C512	Due Diligence	**Effective**	R04
C601	Change Management	**Effective**	R03
C703	Security Tests and Audit Controls	**Effective**	R03
C704	User Training	**Effective**	R02, R03
C705	Awareness Training	**Effective**	R02

2.2 Recommendations

The following table lists the risks identified as part of this assessment and associated recommendations to achieve Target Risk. Three (3) remediation activities have been recommended to improve the effectiveness of the controls for Azure.

ID	Control	Control Title	Recommendation	Related Risks
Rem01	C107	Password Policy	s9(2)(k) [redacted]	R02
Rem02	C203	Business Continuity	Te Puni Kōkiri should s9(2)(k) [redacted]	R04
Rem03	C502	Documentation	s9(2)(k) [redacted]	R03

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Section 3. Risk Acceptance

It is recommended that you:

- **Accept** that the current risks, target risks, and recommendations identified in this report are accurate and appropriate.

Name, Job Title, Puni
Date:_____ ACCEPTS RISKS / DOES NOT ACCEPT

Name, Job Title, Puni
Date:_____ ACCEPTS RISKS / DOES NOT ACCEPT

RELEASED UNDER THE OFFICIAL INFORMATION ACT

8

Section 4. Context

4.1 Solution Overview

Microsoft offers Azure as subscription based infrastructure services that allow the customer to build or move their physical infrastructure into a virtual environment (the cloud). Azure services are hosted by Microsoft who manage the infrastructure layer and resources via global datacentres, which are shared through a multi-tenancy model. These cloud offering provide virtualised compute, storage and networking environments that can be created or upgraded without physical intervention from the customer.

4.2 Business Impact

What information is contained within the system, what would happen if it was compromised, unavailable or modified.

4.2.1 Information Classification

Azure is certified to the maximum information classification of **IN-CONFIDENCE** and below, based on the Protective Security Requirements (PSR) New Zealand Government Security Classification System. s(9)(2)(k) [redacted] Te Puni Kōkiri do not hold or collect information requiring NZEO controls protection.

4.2.2 Confidentiality

The impact of any confidentiality breach would be considered **MAJOR** to Te Puni Kōkiri. This is due to the nature of the information contained within and passing through components of Azure containing Personally Identifiable Information (PII). Any breach of PII would result in breaches of legislation including the Privacy Act and would attract widespread media criticism.

4.2.3 Integrity

The impact of a breach of integrity of Azure would be considered **MAJOR** to Te Puni Kōkiri. Due to the strategic and operational risks associated with the use of Azure, a loss of integrity via the use and configuration of Azure could result in inconvenience and negative impact on the achievement of strategic objectives of Te Puni Kōkiri.

4.2.4 Availability

Azure is a service that requires high availability at Te Puni Kōkiri. The impact of the service being unavailable would be considered **MAJOR**. The operational consequences would result in a major degradation of operations and service delivery and require senior management intervention.

4.2.5 Privacy

A Privacy Impact Assessment (PIA) has been completed in 2019 for the use of both M365 and Azure at Te Puni Kōkiri accepting that the principles of the Privacy Act have been considered and configuration is accordance of the principles of the Privacy Act. It is recommended that an updated PIA is undertaken for Azure at the next Certification and Accreditation cycle.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Section 5. Review Details

5.1 Introduction

The focus of this SRA and CVA is the Azure services being consumed by Te Puni Kōkiri. This assessment focuses solely on the risks and controls within the sphere of responsibility of Te Puni Kōkiri, based on their own business context, risk environment and risk appetite. Baseline security assurance for the use of Azure has been undertaken by Lead Agency, and a Service Security Certificate has been issued until 30 June 2025.

A Cloud Risk Discovery Assessment has also been undertaken, and a copy of this is available here:
2024 05 01 IS Cloud Risk Discovery Tool Azure.xlsm

5.2 Approach

As part of this assessment the following documents were reviewed:

- 2024 05 01 IS Azure Cloud and Azure AD Service Security Certificate v1.0.pdf
- 2024 05 01 IS Microsoft Azure and Azure Active Directory Security Risk Assessment Report.pdf
- 2019 02 19 CN Privacy Impact Assessment (signed).pdf

Additionally, technical and process correspondence was exchanged with Willem Loots, Lead Cloud Engineer - Organisational Support Technology & Systems.

Evidence discovery was undertaken to confirm Te Puni Kōkiri configuration of the Azure instance, and screenshots of evidence collected is located here:

5.3 Scope

Items within scope:

- Azure Cloud Services, including Azure Virtual Machines, Azure Storage, Azure Key Vault
- Azure Active Directory Services

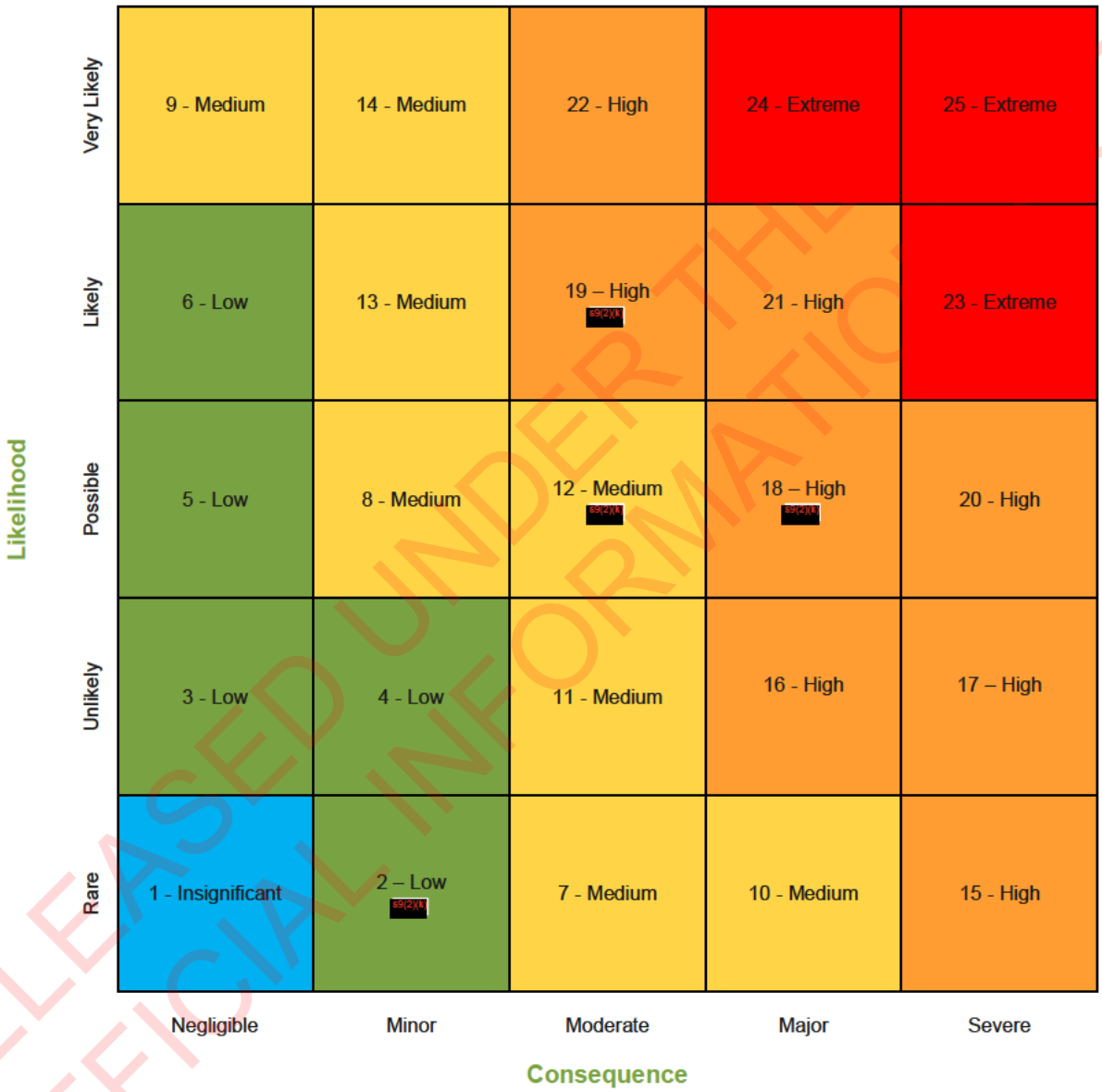
Items out of scope:

- Applications that are hosted on Azure infrastructure
- Connectivity, networking or interfaces between Azure infrastructure and other services or applications
- Any items not included in the in-scope items listed above

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Section 6. Current Risk Matrix

This table demonstrates the risk to the business with current (assessed) controls only. These are controls that are already present in the current IT environment.



R01: Inadequate Protection of Data in Transit and at Rest

R02: Unauthorised Access to Systems

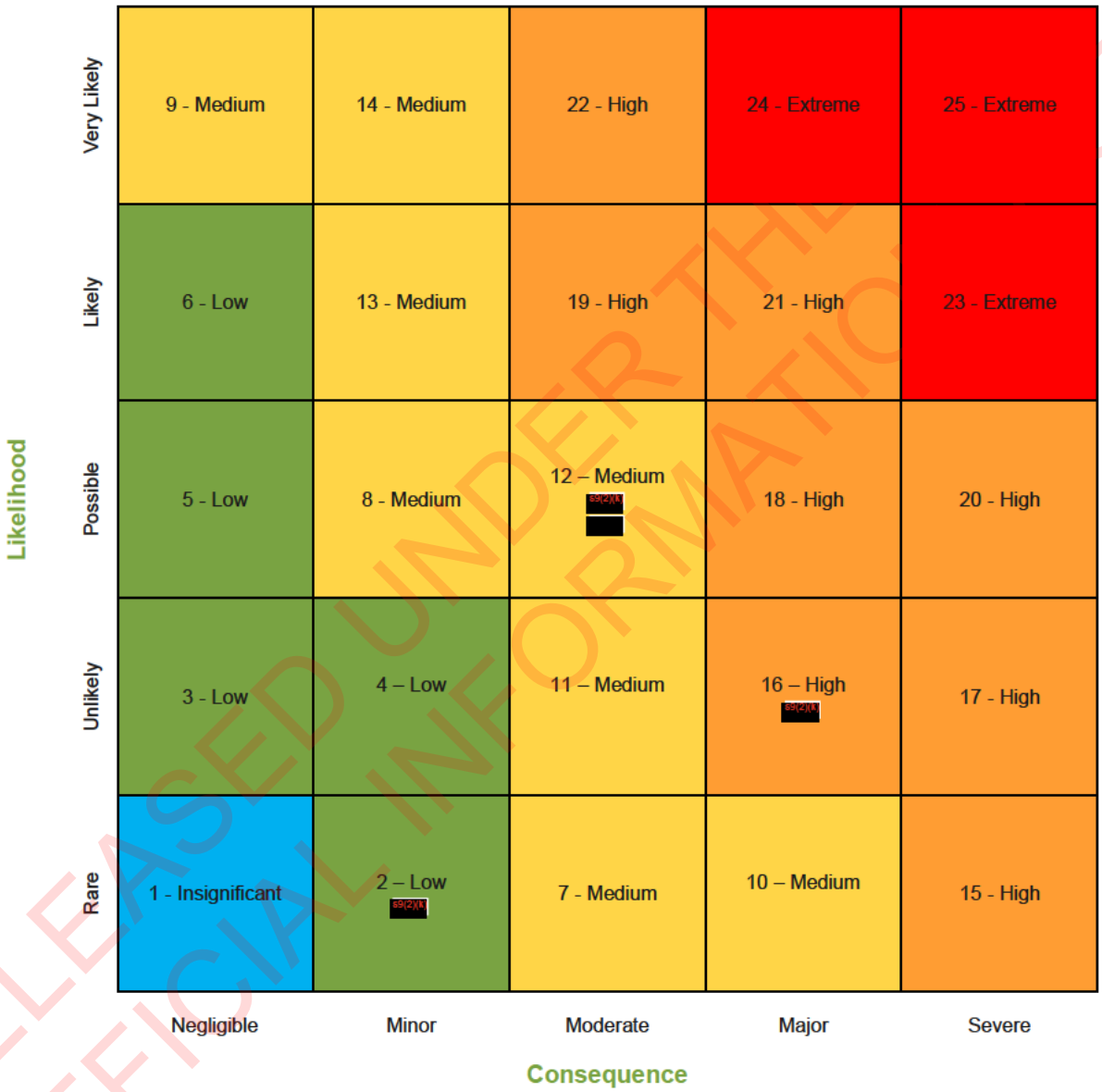
R03: Misconfiguration of Azure

R04: Data Sovereignty and Jurisdictional Risk

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Section 7. Target Risk Matrix

This table demonstrates the expected remaining risk to the business if all the recommended controls are implemented effectively.



R01: Inadequate Protection of Data in Transit and at Rest

R02: Unauthorised Access to Systems

R03: Misconfiguration of Azure

R04: Data Sovereignty and Jurisdictional Risk

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Section 8. Detailed Risk Findings

This section provides an itemised list of risks, associated controls, and risk levels as they would apply with no controls (Current Risk – as per the Risk Table above), and risk levels with all controls properly implemented (Target Risk – as per the Risk Table above).

Risk ID	Description	Current Risk	Controls	Target Risk
R01	**Inadequate Protection of Data in Transit and at Rest** Azure is a cloud-based solution and is internet facing. Te Puni Kōkiri data both at rest and in transit could be accessed by unauthorised individuals. This could lead to: • Information is disclosed, modified, or deleted. • Disruption to business processes. • Reputational damage. • Legislative and regulatory failure. • Loss of trust from key stakeholders. **Example scenarios & triggers:** s9(2)(k) [redacted]	s9(2)(k) [redacted]	C401 – Data Encryption in Transit C402 – Data Encryption at Rest C406 – Security Information and Event Management (SIEM) C407 – Event Logging, Monitoring and Auditing C408 – Intrusion Detection and Prevention C503 – Cryptographic Key Management	**Medium (11)**

RELEASED UNDER THE OFFICIAL INFORMATION ACT

R02	**Unauthorised Access to Systems** An unauthorised malicious actor could gain access to the solution due to failures in access control policies and / or authentication. This may lead to: • Information is disclosed, modified, or deleted. • Reputational damage. • Legislative and regulatory failure. • Disruption to business processes. • Unavailability of Azure. **Example scenarios & triggers:** s9(2)(k) [redacted]	s9(2)(k)	C101 – Role Based Access Control C103 – Multi-Factor Authentication C104 – Management of Privileged Access C107 – Password Policy C406 – Security Information and Event Management (SIEM) C407 – Event Logging Monitoring and Auditing C704 – User Training C705 – Awareness Training	**Medium (12)**
R03	**Misconfiguration of Azure** As Azure is cloud based and internet facing, a lot of default settings within the solution are open or public and require configuration to ensure they are configured securely. Misconfigured instances within Azure could expose the Te Puni Kōkiri Azure tenancy to the wider internet, or inability for some systems or services to synchronise with Azure Active Directory.	s9(2)(k)	C101 – Role Based Access Control C104 – Management of Privileged Access C502 – Documentation C601 – Change	**High (16)**

RELEASED UNDER THE OFFICIAL INFORMATION ACT

	This could lead to: • Information is disclosed, modified, or deleted. • Reputational damage. • Legislative and regulatory failure. • Disruption to business processes. • Unavailability of Azure. **Example scenarios & triggers:** s9(2)(k) [redacted]		Management C703 – Security Tests and Controls Audit C704 – User Training	
R04	**Data Sovereignty and Jurisdictional Risk** Microsoft relocates Te Puni Kōkiri Azure instances in their datacentres from the previously agreed region to another without notification or consultation. Expectations and requirements regarding security relating to Te Puni Kōkiri data the need for data contained within the Azure to be only stored within New Zealand and Australia are not clearly defined. This could lead to: • Information is disclosed, modified, or deleted. • Disruption to business processes.	s9(2)(k)	C105 – Information Transfer C203 – Business Continuity C511 – Contracts and Service Level Agreements (SLAs) C512 – Due Diligence	**Low (2)**

RELEASED UNDER THE OFFICIAL INFORMATION ACT

- Reputational Damage.
- Loss of trust from key stakeholders.
- Unavailability of Azure.

Example scenarios & triggers:

s9(2)(k) [redacted]

Section 9. Controls Validation

This section provides an itemised list of controls, a description of how each control works, and the effect each control has on risks.

ID	Title	General Description	Solution Specific Requirement	Applicable Risks	Effect on Risk	Status	Assessment Comments
C101	Role Based Access Control	Access to the service is controlled based on the roles of the individuals requiring access. Role based access controls allows access to be quickly, easily, and uniformly granted, changed, or removed for groups of users, without having to update the privileges for each user. In accordance with the principle of	Kaimahi are granted access to the Azure services based on their role, with administrators holding separate logins. Access is based on the principles of least	R02, R03	Likelihood Impact	**Effective**	**Evidence:** 2024 14 06 IS Azure Evidence Screenshots.docx **Assessment:** Users are created and placed into user groups, with separate security groups giving elevated

RELEASED UNDER THE OFFICIAL INFORMATION ACT

		least privilege, only the minimum required access rights are granted to a user or system when accessing a system, preventing the assignment of excessive user permissions. Privileged access rights are controlled through formal authorisation process and implemented in accordance with the defined access control policy.	privilege.				access rights. Security groups are configured for instances where users require additional access or permissions. Administrative users have separate and distinct logins, and elevated access requests are undertaken via s9(2)(k) [redacted] **Recommendations:** Nil.
C103	Multi-Factor Authentication	Where strong authentication and identity verification is required (e.g. privileged users, administrators) additional forms of authentication can be used (e.g. tokens, digital certificates, biometrics). Multi-factor authentication provides the strongest level of authentication, as it requires a combination of at least two of the following forms of identification: • Something you know (e.g. username and password). • Something you have (e.g. hardware or software token, digital certificate). • Something you are (e.g. biometric fingerprint).	Multi-Factor Authentication is configured for login to Azure portals.	R02	Likelihood Impact	**Effective**	**Evidence:** 2024 14 06 IS Azure Evidence Screenshots.docx **Assessment:** Screenshots from Microsoft Azure confirming that s(9)(2)(k) [redacted] Login tests undertaken as both a standard and privileged user prompted to s(9)(2)(k) [redacted] **Recommendations:** Nil.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

C104	Management of Privileged Access	Control the allocation, maintenance, and removal of privileged access rights to restrict administrative privileges to only the activities that require them and prevent them from being used for business as usual or day-to-day activities. Privileged access rights are controlled through formal authorisation processes and implemented in accordance with an access control policy.	Confirm that Privileged Access policies are configured in Azure.	R02, R03	Likelihood	**Effective**	**Evidence:** 2024 14 06 IS Azure Evidence Screenshots.docx **Assessment:** Privileged access is managed via s(9)(2)(k) [redacted] Administrator logins are created for users that require elevated privileges that are separate to standard production logins. Access is granted via roles on an as required basis to undertake required duties. s(9)(2)(k) [redacted] **Recommendations:** Nil.
C105	Information Transfer	Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organisation and between the organisation and other parties and should follow the requirements of the information classification. Data sovereignty laws and restrictions should be followed as well as the New Zealand Privacy Act (2020).	Data location for Microsoft is confirmed to be configured to geographic locations appropriate for Te Puni Kōkiri data.	R04	Likelihood	**Effective**	**Evidence:** 2024 14 06 IS Azure Evidence Screenshots.docx **Assessment:** Confirmation that the data locations for Te Puni Kōkiri are configured for s(9)(2)(k) [redacted] **Recommendations:** Nil.
C107	Password	Define and implement a password policy to make sure individuals have	Evidence that the password policy is	R02	Likelihood	**Partially**	**Evidence:** 2024 14 06 IS Azure

RELEASED UNDER THE OFFICIAL INFORMATION ACT

	Policy	the right information to help keep their user accounts safe, and the business' networks and systems secure. This could include enforced password changes at regular intervals, and rules to ensure the quality of the passwords created, such as length, special characters, and blacklisted character sequences i.e., the users name, organisation names etc.	configured for Te Puni Kōkiri Azure logins.			**Effective**	Evidence Screenshots.docx **Assessment:** The password policy in force at Te Puni Kōkiri is partially effective. Minimum password length requirement and enforced password age configured. However, s(9)(2)(k) [redacted]. **Recommendations:** s9(2)(k) [redacted]
C203	Business Continuity	Business continuity plans should be established to assist in meeting business requirements, minimise disruption to the availability of information and systems and assist recoverability. By defining the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for the Service, business owners can maintain achievable continuity objectives. Developing and testing a plan confirms appropriate measures are identified and implemented for the continuity of critical business services. Information Security Continuity is an integral component of disaster	A Business Continuity Plan is in place at Te Puni Kōkiri, that has been tested in the past 12 months.	R04	Impact	**Partially Effective**	**Evidence:** 2022 10 14 PL Business Continuity Plan V7 **Assessment:** A detailed Business Continuity Plan for Te Puni Kōkiri is available. It clearly defines roles, processes and procedures across all aspects of the business. s9(2)(k) [redacted] s(9)(2)(k)

RELEASED UNDER THE OFFICIAL INFORMATION ACT

		recovery and business continuity plans. Processes, procedures, and controls should be established, documented, and implemented to achieve the required level of information security. This includes adequate management structure with the necessary authority and incident response teams to act in case of disasters, as well as all the necessary controls required. As with all information security documentation, these processes need to be periodically verified, reviewed, tested, and evaluated to make sure it meets the outlined requirements.					s(9)(2)(k) [redacted] **Recommendations:** Te Puni Kōkiri should keep a record of testing of the Business Continuity Plan and ensure testing is conducted annually. s(9)(2)(k) [redacted] for Information Security or an addendum plan created for Information Security Business Continuity.
C401	Data Encryption in Transit	Sensitive business, private, or otherwise classified information in transit is always protected using approved cryptographic protocols, reducing the likelihood of information being disclosed to, or captured by, an unauthorised person.	Data in Transit through Azure tenancy is encrypted.	R01	Likelihood	**Effective**	**Evidence:** 2024 14 06 IS Azure Evidence Screenshots.docx **Assessment:** Data in Transit is s(9)(2)(k) [redacted] **Recommendations:** Nil.
C402	Data Encryption at Rest	Sensitive business, private or otherwise classified information must be encrypted in storage, or at rest, using approved encryption algorithms and protocols. This reduces the	Data at Rest in Azure tenancy is encrypted.	R01	Likelihood Impact	**Effective**	**Evidence:** 2024 14 06 IS Azure Evidence Screenshots.docx

RELEASED UNDER THE OFFICIAL INFORMATION ACT

		likelihood and impact of information disclosure in cases where malicious actors gain access to storage media, logically or physically.					**Assessment:** Data at Rest in the Azure tenancy is encrypted using s9(2)(k) and encryption keys are stored using s9(2)(k) **Recommendations:** Nil.
C406	Security Information and Event Management (SIEM)	Implementing a Security Information and Event Management (SIEM) solution that is capable of log aggregation and correlation that can automatically detect and alert on selected events in real-time will provide the organisation with additional security. Many SIEM solutions can detect abnormal behaviour patterns (e.g., identification of numerous user accounts being locked out, indicating a user account enumeration and/or a brute force password attack is underway). Additionally, a SIEM solution can be implemented to reflect normal business processes and alert on security logs that do not conform with business-as-usual. Security Orchestration, Automation and Response (SOAR) technologies or a Security Operations Centre (SOC) environment can increase the effectiveness of the SIEM.	A SIEM solution is in place at Te Puni Kōkiri.	R01, R02	Likelihood	**Effective**	**Evidence:** 2024 14 06 IS Azure Evidence Screenshots.docx **Assessment:** Te Puni Kōkiri utilise both s9(2)(k) to monitor and log events across their tenancy. Logging is aggregated and ingested into s(9)(2)(k) s9(2)(k) **Recommendations:** Nil.
C407	Event Logging, Monitoring and Auditing	Systems are configured with adequate logging and that the logs are archived and retained for a defined appropriate period. Current best practice	Logging and monitoring is implemented and configured across	R01, R02	Likelihood Impact	**Effective**	**Evidence:** 2024 14 06 IS Azure Evidence Screenshots.docx

RELEASED UNDER THE OFFICIAL INFORMATION ACT

		guidelines recommend logging the following activities and information: • User login. • All privileged operations. • Failed attempts to elevate privileges. • Security related system alerts and failures. • System user and group additions, deletions, and modification to permissions. • Unauthorised or failed access attempts to systems and files identified as critical to the agency. • Date and time of the event. • Relevant system user(s) or processes. • Event description. • Success or failure of the event. • Event source (e.g. application name). • IT equipment location/identification. Security related event logs are analysed regularly using automated security information and event management (SIEM) tools or equivalent to help identify anomalies.	the Te Puni Kōkiri Azure tenancy.				**Assessment:** Te Puni Kōkiri utilise both s9(2)(k) to monitor and log events across their tenancy. s9(2)(k) [redacted] **Recommendations:** Nil.
C408	Intrusion Detection and Prevention	Intrusion Detection and Prevention monitors network and/or system activities for malicious activity. The main functions are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it. They can be deployed in three ways:	Intrusion Detection and Prevention is implemented and configured for the Azure tenancy.	R01	Likelihood Impact	**Effective**	**Evidence:** 2024 14 06 IS Azure Evidence Screenshots.docx **Assessment:** Te Puni Kōkiri utilise both s9(2)(k) to monitor and log

RELEASED UNDER THE OFFICIAL INFORMATION ACT

		• Network-Based Intrusion Prevention System (NIPS): monitors the entire network for suspicious traffic by analysing protocol activity. • Wireless Intrusion Prevention Systems (WIPS): monitor a wireless network for suspicious traffic by analysing wireless networking protocols. • Network Behaviour Analysis (NBA): examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware and policy violations.					events across their tenancy. s(9)(2)(k) [redacted] **Recommendations:** Nil.
C502	Documentation	Documenting systems, assets and processes help share information between stakeholders and prevent human error related mistakes. The following documents are considered best practice: • Sufficient design and technical documentation to support the rebuilding of information services and systems. • Security Risk Management Plans – identifying security risks and appropriate treatment measures for systems. • System Security Plans – specifying the information security measures for systems. • Emergency Procedures – ensuring classified information and systems are secured before personnel evacuate a facility in the event of an emergency.	Appropriate documentation for Azure implementation and use has been created.	R03	Likelihood Impact	**Partially Effective**	See intranet links in section 10.1 below. **Assessment:** Te Puni Kōkiri has a comprehensive library of system documentation and policies. Enterprise level documentation for policy and process is detailed, but in some instances is either s(9)(2)(g)(i) [redacted] . s(9)(2)(k) [redacted] however aspects are

RELEASED UNDER THE OFFICIAL INFORMATION ACT

							covered in the overarching documentation. **Recommendations:** s(9)(2)(k) [redacted] the Te Puni Kōkiri tenancy, including any role specific user guides. Completion of outstanding documentation reviews.
C503	Cryptographic Key Management	Cryptographic keys are managed according to defined standards and procedures and protected against unauthorised access or destruction during their lifecycle, including creation, storage and protection, distribution, use, renewal, recovery, revocation, destruction.	Confirmation that Cryptographic Keys are managed effectively.	R01	Likelihood	**Effective**	**Evidence:** 2024 14 06 IS Azure Evidence Screenshots.docx **Assessment:** Te Puni Kōkiri s(9)(2)(k) [redacted] and access is restricted to only specified administrative users. **Recommendations:** Nil.
C511	Contracts and Service Level Agreements	Contracts and Service Level Agreements (SLAs) are clearly defined and reviewed to be in line with information security requirements. They should also have appropriate measures in place to meet the level of availability and performance required. Non-Disclosure Agreements (NDA) can be written to prevent contractors or other individuals from sharing	SLAs have been defined and are in line with Te Puni Kōkiri agreements.	R04	Likelihood	**Effective**	**Evidence:** 2024 14 06 IS Microsoft Online Service SLAs.docx **Assessment:** Microsoft have produced a listing of SLAs for all services across their Cloud offerings which outlines their obligations under the licencing

RELEASED UNDER THE OFFICIAL INFORMATION ACT

		sensitive information.					agreement between Microsoft and Te Puni Kōkiri. The SLAs detail uptime targets and penalties for not meeting these targets. **Recommendations:** Nil.
C512	Due Diligence	Adequate due diligence is done for suppliers and vendors to identify and manage any third-party dependencies, manage potential supply chain risks, and define information security requirements. This can include: • Identifying in which country the data could be processed, transmitted and / or stored in. • Clearly defining the legal jurisdiction for contractual disputes relating to the use and function of the Service. In projects where development is outsourced, the organisations required security measures still to be maintained through directing, monitoring, and reviewing actions taken by outsourced developers.	Confirmation that Te Puni Kōkiri have configured their Azure tenancy geographic location for data storage to a region that is appropriate.	R04	Likelihood Impact	**Effective**	**Evidence:** 2024 05 01 IS Cloud Risk Discovery Tool Azure.xlsm 2024 05 01 IS Azure Cloud and Azure AD Service Security Certificate v1.0.pdf 2024 05 01 IS Microsoft Azure and Azure Active Directory Security Risk Assessment Report.pdf **Assessment:** s(9)(2)(k) [redacted], which is the best current available storage region for Microsoft products. As Azure is an All of Government certified product, Due Diligence requirements are met by Azure Cloud Services and Azure Active Directory having been issued a Security Certificate, and Te Puni Kōkiri undertaking a review of the Risk

RELEASED UNDER THE OFFICIAL INFORMATION ACT

							Assessment Report that is produced and complying with the Consuming Agency requirements recommended in the report. **Recommendations:** Nil.
C601	Change Management	Changes to a system should be documented and approved through a formal change control process. All changes unsuccessful and partially successful should be reviewed.	A change control process has been documented and is in use at Te Puni Kōkiri.	R03	Likelihood Impact	**Effective**	**Evidence:** 2022 07 09 FN Change Control Process and Template.docx **Assessment:** The Change Control Process and Template document details the change control process in place at Te Puni Kōkiri, along with defining the types of changes (Emergency, Standard, Non-Standing) that could be required. The review process for changes is defined, along with the roles responsible for the change. **Recommendations:** Nil.
C703	Security Tests and Audit Controls	Information assurance activities such as controls audit and technical security assessments are conducted against systems to demonstrate that due consideration has been paid to risk, security, functionality, business requirements and as a fundamental part of information systems	Assurance activities are undertaken for Azure use and implementation at Te Puni Kōkiri.	R03	Likelihood Impact	**Effective**	**Evidence:** 2024 05 01 IS Cloud Risk Discovery Tool Azure.xlsm 2024 05 01 IS Azure Cloud and Azure AD Service Security Certificate v1.0.pdf 2024 05 01 IS Microsoft

RELEASED UNDER THE OFFICIAL INFORMATION ACT

		governance and assurance. The assurance activities should focus on validating whether: • Security posture of the organisation has been incorporating into its system security design • Controls are correctly implemented and are performing as intended • Changes and modifications are reviewed for any impact or implications • Effectiveness of information security measures for systems is periodically reviewed and validated. Penetration tests (when allowed and carried out by a reputable third-party), also provide assurance that exploitable information system weakness is identified, controls are configured and enforced to protect against real world attack scenarios.					Azure and Azure Active Directory Security Risk Assessment Report.pdf **Assessment:** s(9)(2)(k) [redacted] issued by Lead Agency which forms part of the overarching Certification and Accreditation of Azure. Te Puni Kōkiri have undertaken a Cloud Risk Assessment of Azure and this Security Risk Assessment and Controls Validation document forms part of the ongoing recertification of Azure for use at Te Puni Kōkiri. **Recommendations:** Nil.
C704	User Training	Organisation and third-party staff that are users or administrators receive formal training on how to perform the tasks that are relevant to their role before they are granted access to the information services.	User training systems and processes are implemented at Te Puni Kōkiri.	R02, R03	Likelihood Impact	**Effective**	**Evidence:** Pūnaha Ako Course Catalogue **Assessment:**. Kaimahi at Te Puni Kōkiri have access to a comprehensive course catalogue for e-learning via Pūnaha Ako. Microsoft training is encouraged to be undertaken by kaimahi within the Technology and Systems team. **Recommendations:**

RELEASED UNDER THE OFFICIAL INFORMATION ACT

							Nil.
C705	Awareness Training	Provide all employees and contractors with ongoing security / privacy awareness training. Topics such as information security responsibilities, legislation and regulation, consequences of non-compliance with information security policies and procedures and potential security risks and counter measures should be covered.	Awareness training is available for kaimahi at Te Puni Kōkiri.	R02	Likelihood	**Effective**	**Evidence:** Pūnaha Ako Course Catalogue **Assessment:**. Te Puni Kōkiri have developed an extensive suite of e-learning modules via Pūnaha Ako. Kaimahi receive training in all areas prescribed as part of the New Zealand Government Protective Security Requirements and Information Security. **Recommendations:** Nil.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Appendix

10.1 References

The following documents are referred to in the memo above, and details including location are noted in the table below.

Document Title	Date	Evidence
2024 05 01 IS Cloud Risk Discovery Tool Azure.xlsm	01/05/2024	s9(2)(k) [redacted]
2024 05 01 IS Azure Cloud and Azure AD Service Security Certificate v1.0.pdf	31/08/2022	s9(2)(k) [redacted]
2024 05 01 IS Microsoft Azure and Azure Active Directory Security Risk Assessment Report.pdf	30/08/2022	s9(2)(k) [redacted]
2019 02 19 CN Privacy Impact Assessment (signed).pdf	19/02/2019	s9(2)(k) [redacted]
2024 14 06 IS Azure Evidence Screenshots.docx	14/06/2024	s9(2)(k) [redacted]
2022 10 14 PL Business Continuity Plan V7	14/10/2022	s9(2)(k) [redacted]
2024 14 06 IS Microsoft Online Service SLAs.docx	14/06/2024	s9(2)(k) [redacted]
2022 07 09 FN Change Control Process and Template.docx	09/07/2022	s9(2)(k) [redacted]
Link for Policies Register		s9(2)(k) [redacted]
Link for Information Technology Policies		s9(2)(k) [redacted]
Link for Pūnaha Ako		s9(2)(k) [redacted]

10.2 Escalation of Risk

The table below provides an example of risk escalation and reporting. It defines who must be informed and has authority to accept risk based on its magnitude.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Note that the below table needs to be referred/approved to the Risk Team

	Risk Escalation and Reporting Level for Each Level of Risk
Very High	Chief Executive
High	Senior Leadership Team
Medium	Business Owner
Low	Service Manager or Project Manager
Insignificant	Service Manager or Project Manager

RELEASED UNDER THE OFFICIAL INFORMATION ACT

10.2 Impact Assessment

The qualitative scale used to assign impact ratings is presented in the table below.

Rating	Political Risks Risks that could impact our decision on reputation and credibility	Strategic Risks Risks that could affect our ability to achieve the outcomes of strategic direction and priority areas	Operational Risks Risks that could impact on our business processes and technology that enables them	Financial Risks Risks that could affect the ability to meet our financial obligations and use value-for-money reasoning	People Risks Risks that could affect the safety and well-being of our people	Legal Risks Risks that could affect our compliance with internal and external expectations including meeting our legal obligations
5 - Severe	Widespread media and public criticism of the Minister(s), Prime Minister and government in general	Inconvenience and impact on the achievement of outcomes where failure is inevitable	Widespread and total degradation of operations or service delivery. Long term doubt about sustainable operations and immediate senior management intervention required	Exceeds 5% of budget / appropriations	Would cause loss of life	Significant prosecution and fines. Very serious litigation
4 - Major	Widespread media and public criticism of the Minister(s)	Inconvenience and impact on the achievement of outcomes to a point where success is questionable	Major degradation of operations or service delivery. Senior management intervention required	Does not exceed 5% of budget / appropriations	Would cause serious casualties resulting in long term physical impairment of our people	Major breaches of regulation. Major litigation and fines possible
3 - Moderate	Selective media criticism of the Minister(s)	Major inconvenience and impact on the achievement of outcomes with an impact on schedule and cost	Serious degradation of operations or service delivery. Local management intervention required with national resources	Does not exceed 3% of budget / appropriations	Would cause several casualties that require hospitalisation with no long-term effects	Moderate breaches. Possibility of being fined
2 - Minor	Minimal criticism of	Minor inconvenience or impact on the	Significant degradation of	Does not exceed 1% of budget /	Would cause several minor casualties that	Minor legal issues, non-compliances, or

RELEASED UNDER THE OFFICIAL INFORMATION ACT

	the Minister(s)	achievement of outcomes with minor impact on schedule	operations or service delivery. Local management intervention required with local resources	appropriations	require medical attention off-site with no long-term effects	breaches of regulation
1 - Negligible	No criticism of the Minister(s)	Minor inconvenience or impact on the achievement of outcomes and no impact on schedule	No measurable operational impact on Te Puni Kōkiri	Does not exceed 0.1% of budget / appropriations	Would cause minor injuries that are able to be treated onsite with no long-term effects	Negligible non-compliances or breaches of regulation

10.3 Likelihood Assessment

The qualitative scale used to assign a likelihood rating is presented in the table below. Where information is available about the frequency of an incident in the past it should be used to determine the likelihood of the risk eventuating. However, where such information does not exist it does not necessarily mean that the likelihood of the risk eventuating is low. It may merely indicate that there are no controls in place to detect it or that the business has not previously been exposed to the risk.

Rating	Description	Definition
5	Very Likely	Likely to occur more than once a year
4	Likely	Likely to occur between once a year and once every two years
3	Possible	Likely to occur between once every two years and once every five years
2	Unlikely	Likely to occur between once every five years and once every ten years
1	Rare	Likely to occur less than once every ten years

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Te Puni Kōkiri
MINISTRY OF MĀORI DEVELOPMENT

Te Puni Kōkiri, Te Puni Kōkiri House, 143 Lambton Quay, PO Box 3943, Wellington, New Zealand
PHONE Waea 0800 875 663 (0800 TPK MMD), **FAX** Waea Whakaahua 0800 875 329 (0800 TPK FAX)
WEB tpk.govt.nz, **FACEBOOK** facebook.com/tepunikokiri

RELEASED UNDER THE OFFICIAL INFORMATION ACT

FORM A - PRIVACY IMPACT ASSESSMENT FORM

"Personal information" held by Te Puni Kōkiri must be protected and dealt with in accordance with the Privacy Act 2020. "Personal information" is defined in the Privacy Act as *"information about an identifiable individual".* As well as identifiers such as a person's name or email address, less obvious examples such as age or employment status fall within this definition if the way the information is recorded identifies the individual. To ensure that Personal Information in Te Puni Kōkiri is handled in accordance with the Privacy Act, could you please complete the following assessment for your area of work.

Microsoft Copilot
Describe the project. Te Puni Kōkiri has not authorised or endorsed the use of Generative AI or Large Language Models for official use. However, we are aware that some kaimahi are using Microsoft Copilot, formerly called Bing Chat Enterprise (BCE). This PIA is being done to ensure that appropriate processes/systems/understandings are in place to protect personal information when kaimahi are engaging with Copilot. *Name of person responsible for the project* Richard Foy, Manager Knowledge Systems is leading work in relation to Microsoft Copilot, Generative AI and Large Language Models
What is the project aiming to achieve and how will it support TPK's work? Microsoft Copilot, formerly known as Bing Chat Enterprise, is an AI-powered chatbot designed for use in business organisations. Copilot (unlike the public Bing Chat that comes as default with the Microsoft Edge browser) has Commercial Data Protection. According to Microsoft: ▪ User and business data in Copilot is protected and will not leak outside the organization. ▪ Chat data is not saved, and Microsoft has no eyes-on access to it. ▪ Additionally, chat data is not used to train the underlying models. Copilot could be used by kaimahi to: ▪ Wordsmith a document. ▪ Suggest potential content for a report or document. ▪ Summarise a long document. ▪ Suggest research sources.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Will new personal information be collected or will the project use information we currently hold? Kaimahi could potentially input personal information into Copilot as part of their query. Copilot could potentially source personal information from its own search database and provide this personal information in its response to kaimahi queries. *How long will the project be in place and personal information be required?* Copilot is being used in BAU. Kaimahi will be made aware of, and be expected to comply with, their privacy obligations (under TPK's Personal Information Policy and Processes) in relation to any personal information Copilot may provide in response to their queries.

COLLECTION STAGE		
Privacy Act Requirements	**Questions**	**Answers**
TPK can only collect personal information, for a purpose that is related to a lawful function of TPK *and* the personal information must be necessary for the purpose TPK wants to achieve.	What is the purpose for which the Personal Information being/likely to be collected using Copilot? Is this purpose a lawful function of TPK? What Personal Information is being/likely to be collected using Copilot? Is TPK aware of the data sources Copilot is trained on and how reliable these sources are for our purposes? What assurances do you have that Copilot will provide accurate and reliable Personal Information. What steps are being taken to minimise any risks to Personal Information associated with the use of Copilot and the risk of privacy breaches?	Kaimahi have been given interim guidance to not use large language model AI technology for work purposes until there is more understanding of the risks associated with AI. (https://intranet.te-wheke.int/en/guides-and-tools/technology/guidelines-for-using-chatgpt). This would include using Copilot to collect personal information. Additionally, kaimahi have been given guidance that they need to be wary of entering any personal information into Copilot. This guidance points to our Personal Information Policy. (https://intranet.te-wheke.int/en/whats-on/kotuitui/chatgpt-to-use-or-not-to-use-find-out). However, we have been unable to turn off the AI chat feature in Microsoft Edge browser and realise that kaimahi may use it if it is readily available to them in a work tool. For this reason, we recognise additional guidance will be required to be given.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

		The most likely use of Copilot within Te Puni Kōkiri would be to aid in writing documents, such as: - wordsmithing - suggesting possible content - finding out more about a particular topic This use of Copilot is certainly within the lawful function of Te Puni Kōkiri. TPK does not know what training datasets are being used to train Copilot. That information is not publicly available. We will be instructing kaimahi not to input personal information in their queries, nor to ask for personal information about individuals. If they ever have a valid use case to do so, they will be required to complete a separate PIA for that purpose. We can not make any assurances that any information Copilot provides will be accurate or reliable. As with any research on the Internet, any information received must be double-checked and assessed for accuracy. We will update the interim guidance to kaimahi to take into account the availability of Copilot, place notices on the Intranet and inform Managers directly of these matters as well.
In general, personal Information needs to be collected directly from the individual concerned and	Does Copilot use publicly available information to respond to queries?	We do not know what datasets have been used to train Copilot in order for it to provide information.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

the individual must be informed of the following (Disclosure and Consent Process): • That the information is being recorded; • How it is being recorded (electronic and/or hard copy); • The purpose it is being collected for; • Name and address of Agency collecting and the Agency that will hold the information. • Whether supplying the information is voluntary; • Consequences if request for information is declined; • Who will be able to access and use the information; • That the individual has the right to access and to ask to have the information corrected; and • The information will be destroyed once it is no longer needed. An exception to this rule is where the personal information is publicly available.	If the answer to the above is 'no' then kaimahi have to obtain Consent Form from Legal Services for the individual to sign before their personal information is shared with you.	We can assume that large portions of the datasets are publicly available information. Microsoft have indicated that any information used in prompts or queries within our Bing Chat Enterprise is not retained and not added to the training dataset used by Microsoft for its AI. Consequently any personal information contained in any queries will not be retained. (https://learn.microsoft.com/en-us/copilot/privacy-and-protections). However, we will be instructing kaimahi not to input personal information in their queries, nor to ask for personal information about individuals. If they ever have a valid use case to do so, they will be required to complete a separate PIA for that purpose. We will update the interim guidance to kaimahi to take into account the availability of Copilot, place notices on the Intranet and inform Managers directly of these matters as well.

USE STAGE		
If TPK staff are using Copilot to collect personal information they must be made aware of the Personal Information Policy	What steps have been taken to ensure that kaimahi handling this personal information have been made aware of the Personal Information Policy requirements and the Collection Use processes?	Kaimahi should not be using Copilot to collect personal information. If they have a valid use case to do so, they should be instructed to fill in a separate PIA for that purpose. This will ensure

RELEASED UNDER THE OFFICIAL INFORMATION ACT

requirements and the Collection Processes above.		that appropriate steps are taken to protect personal information. Our interim guidelines will be updated to address the privacy aspect of using Copilot. We will also be placing notices on the Intranet and informing Managers directly of these matters as well.
TPK cannot repurpose personal information it holds for a new purpose unless it is a directly related purpose, authorised by laws or a specific exemption under the Privacy Act applies.	What steps have been taken to ensure that kaimahi handling this personal information have been made aware of the Personal Information Policy requirements and the Collection Use processes?	Kaimahi should not be using Copilot to collect personal information or repurpose any personal information that comes to them. If they ever have a valid use case to do so, they should be instructed to fill in a separate PIA for that purpose. This will ensure that appropriate steps are taken to protect personal information. Our interim guidelines will be updated to address this privacy aspect of using Copilot. We will also place notices on the Intranet and inform Managers directly of these matters as well.
If a third party is collecting the information for TPK then TPK must take reasonable steps to ensure that they comply with the privacy Act too.	Does Copilot use publicly available information for collecting personal information when kaimahi send a request through. If the answer to the above is 'no' then what steps have been taken to: • Require Copilot to comply with the Privacy Act; and • require that Copilot confirm that it has Privacy Act compliant processes in place for the collection, use, storage, and disclosure of the information?	We do not know what datasets have been used to train Copilot in order for it to provide information. We can assume that large portions of the datasets are publicly available information. Microsoft have indicated that any information used in prompts or queries within our Bing Chat Enterprise is not retained and not added to the training dataset used by Microsoft for its AI. (https://learn.microsoft.com/en-us/copilot/privacy-and-protections).

RELEASED UNDER THE OFFICIAL INFORMATION ACT

		However, we would certainly advise kaimahi not to input personal information in their queries, nor to ask for personal information about individuals. If they ever have a valid use case to do so, they should be instructed to fill in a separate PIA for that purpose. This will ensure that appropriate steps are taken to protect personal information. We will also update the interim guidance to kaimahi to take into account the availability of Copilot, place notices on the Intranet and inform Managers directly of these matters as well.
The Act requires Personal Information to be collected directly from the person themselves unless TPK has reasonable grounds to believe that the individual has authorised someone else to disclose their personal information to TPK.	Does Copilot use publicly available information to respond to queries ? If the answer to the above is 'no' then what steps have been taken to ensure that the individual has authorised the disclosure of their information by someone else?	As previous question.

ACCESS AND STORAGE STAGE		
Privacy Act Requirements	**Question**	**Answer**
Personal Information is classified as *"In Confidence"* information under TPK's Classified Information Policy. So, the following steps must be taken in relation to the hard copy files and any databases on which personal information is held:	If Copilot provides Personal Information in response to kaimahi queries, where will the Personal Information be held? Who will have access to the Personal Information provided by Copilot in response to queries?	No information received via Copilot is retained within Copilot itself. It relies on kaimahi copying and pasting the information to another source such as a Word document. (https://learn.microsoft.com/en-us/copilot/privacy-and-protections).

RELEASED UNDER THE OFFICIAL INFORMATION ACT

• Electronic files must be protected against illicit internal use or intrusion by external parties in accordance with Te Puni Kōkiri's Records Management Policy, Records Management Guide and Electronic Communication Policy. • Paper documents must be stored in accordance with Te Puni Kōkiri's Records Management Policy and Records Management Guide. • A list of authorised users will be approved by the responsible manager.	How will the Personal Information provided by Copilot be secure against loss or misuse? Where Personal Information provided by Copilot is to be held in a register, database or central file, has a list of "Authorised Users" been approved by the responsible manager? Has access to the centralised file/database/register been restricted to those who "*need to know*"? What steps have been taken to ensure that kaimahi who provide or obtain Personal Information through Copilot are aware of these privacy requirements?	Kaimahi will need to handle any such document according to Te Puni Kōkiri's Security Classification Policy, just as they would for any other document. Kaimahi should not be using Copilot to collect personal information. If they ever have a valid use case to do so, they should be instructed to fill in a separate PIA for that purpose. This will ensure that appropriate steps are taken to protect personal information. We will also update the interim guidance to kaimahi to take into account the availability of Copilot, place notices on the Intranet and inform Managers directly of these matters as well.
"Unique Identifiers" can be used to protect the names of individuals and remove the "privacy" implications. For example, recording information alongside a reference number as a unique identifier rather than a name might make the individual unidentifiable. Care should be taken about adopting a unique identifier unless it is necessary to carry out the purpose efficiently. An identifier assigned by another Agency *(such as an IRD number) should not be used. Using alternative references such as "the client" might make the individual unidentifiable.	Will unique identifiers be assigned to Personal Information obtained or shared with Copilot? Why is this being done and what is the "unique identifier" system that is being proposed?	No unique identifiers are required for the use of Copilot.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

The Act requires that: • Personal Information be kept up to date and accurate; and • individuals be able to access and correct personal information TPK holds about them. So, processes need to be in place to allow access and changes to Personal Information.	What processes have been put in place to ensure that: a. Kaimahi are aware of the data sources that Copilot is trained on; b. Personal Information obtained through Copilot and held by TPK is accurate; c. Individuals can access their information provided by Copilot and request changes? and d. Only authorised changes are made to the information? What steps have been taken to ensure that kaimahi have been made aware of this requirement?	Copilot is not a place where kaimahi can "store" personal information or any information. It can only be queried, and information received, similar to searching on Google. There is no way in which information can be accessed and corrected, but misinformation can be reported to Microsoft. (https://www.microsoft.com/en-nz/concern/bing). As previously mentioned, we have no way of knowing what datasets have been used to train Copilot in order for it to provide information. We will be instructing kaimahi not to input personal information in their queries, nor to ask for personal information about individuals. If they ever have a valid use case to do so, they will be required to complete a separate PIA for that purpose. This will ensure that appropriate steps are taken to protect personal information.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

USE STAGE		
Privacy Act Requirements	**Question**	**Answer**
If the Personal Information is to be used for another purpose (i.e. not the purpose for which it was collected) then the consent of the individual must be obtained: a. the responsible manager must approve the individual being approached for the new purpose; and b. this new consent must be in writing and signed by the individual.	What steps have been taken to ensure that the consent of the individual is obtained before Personal Information is used for another purpose? What steps have been taken to ensure that kaimahi have been made aware of this requirement?	Kaimahi should not be using Copilot to collect personal information or repurposing any personal information that comes to them. If they ever have a valid use case to do so, they should be instructed to fill in a separate PIA for that purpose. Our interim guidelines will be updated to address this privacy aspect of using Copilot.
If you are electronically transmitting any personal information, then you must: a. Double check that the email address that you are sending the information to is correct; b. Add the following statement to the bottom of your email: *"Te Puni Kōkiri is the originating government agency for this email. This email contains personal information which can only be used or disclosed in accordance with the Privacy Act. If you are the intended recipient, then note that this information is disclosed "In-Confidence" and cannot be used for any purpose other than that which Te Puni Kōkiri has disclosed it to you. <u>If you are not the intended recipient of this information, please delete the email from your records</u>*	What steps have been taken to ensure that kaimahi been made aware of this requirement?	Kaimahi should not be using Copilot to collect personal information. If they ever have a valid use case to do so, they should be instructed to fill in a separate PIA for that purpose. Our interim guidelines will be updated to address this privacy aspect of using Copilot.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

and notify the sender by return email that you have received the information in error." a. If you are transmitting Personal Information in paper form, then you must: i. post the information in a single sealed envelope with "*Private - To Be Opened By Addressee Only*" clearly written on the front of the envelope; and ii. include a return address on the envelope in case delivery is unsuccessful. b. If you are disclosing personal information outside New Zealand, seek advice from Legal Services about the terms of TPK's contract with the foreign person or entity. The Privacy Commissioner's website has a model disclosure agreement clause builder. c. If there is no contract between TPK and the foreign person or entity, then you must be satisfied that comparable safeguards or authorisation by the person concerned still apply to disclosure to foreign persons or entitles. You will need to undertake careful checks to be satisfied that you can rely upon this ground. Seek advice from Legal Services before relying on comparable safeguards.		

RELEASED UNDER THE OFFICIAL INFORMATION ACT

DISPOSAL STAGE		
Privacy Act Requirements	**Questions**	**Answer**
Personal information needs to be destroyed once it is no longer required for the authorised purposes. Disposal will need to be done in compliance with TPK's Records Management Policy. You will need to consider: a. Do other laws requiring documents to be retained such as the Public Records Act 2005 apply? b. How long will the information be required for? c. What steps will need to be taken to initiate and complete the disposal process.	How long will the information be required for? What steps have been taken to ensure that Personal Information is destroyed once no longer necessary i.e.: a. Who will initiate the disposal process? b. Who will authorise the actual disposal? and c. Who confirms the information has been destroyed?	*Under the Public Records Act, Te Puni Kōkiri has developed a Disposal Schedule that covers the disposal of personal information. Personal information collected under this project will be disposed of in accordance the Disposal Schedule.*

PIA completed by Signature: _____

Date: _____

Manager Approval:

Date: _____

Legal Clearance

_____ Signature: _____

Solicitor, Legal Services / /

Approved / Not approved

Manaia King Signature: _____

Chief Privacy Officer / /

RELEASED UNDER THE OFFICIAL INFORMATION ACT

RELEASED UNDER THE OFFICIAL INFORMATION ACT

He Pānui

Whakapānga kōnae	LE 18/2/19	**Te Rā**	18 February 2019
Ki a:	Fiona McBeath - Chief Privacy Officer		
Nā:	Beverly Penjueli, Manager Legal Services		
Tauira Pārua:	Colleen Hart, Information Architect, Information Services		
Kaupapa:	**Privacy Impact Assessment – Microsoft AZURE and Office 365**		

Purpose

1. This paper is being submitted to you in your capacity as the Chief Privacy Officer for Te Puni Kōkiri (TPK). It seeks your approval of the attached Privacy Impact Assessment (PIA), for Microsoft AZURE and Office 365 to be used for the storage of emails and data stored on TPK's contents server currently..

Background

2. Under TPK's Personal information Policy and Processes, PIA's are required for new initiatives or reviews of existing initiatives that involve the handling of personal information.
3. Essentially a PIA evaluates a proposal in terms of its impact upon privacy, seeks to identify components of any proposed system that involves the handling of personal information and establishes how the privacy risks associated with that system can be managed.
4. Information Services is proposing to move the storage of emails and data stored on TPK's Contents Server to the cloud. Under this new process:
    - The information will be held in the Cloud on servers provided by Microsoft AZURE;
    - Office 365 will be used to create and edit the documents;
    - The data on the servers is encrypted and can only be accessed by the TPK staff who hold the keys.

Comment

5. The Privacy Act 1993 (the Act) includes information privacy principles that govern the collection, storage, access to, use and disposal of personal information. The attached PIA confirms:
    - No new personal information will be collected as a result of the change;
    - An All of Government Cloud Risk Assessment is being completed to ensure the information will be held securely and administered in accordance with the provisions of the Act. Once completed, the Assessment will be submitted to the Chief Executive for approval;
    - The System makes provision for access to the personal information by TPK staff to be on a need to know basis only;

RELEASED UNDER THE OFFICIAL INFORMATION ACT

- The data stored will be "refreshed" at the end of each business day, which will help to ensure personal information will be disposed of in accordance with the requirements of the Act.

6. I am satisfied that all privacy matters have been adequately addressed, and that processes will be in place to ensure that ongoing privacy matters are adequately provided for.

7. The PIA is in order for signing therefore.

Recommendation

It is recommended that you sign the attached PIA for the transfer of the storage of emails and data to the Cloud as Te Puni Kōkiri's Chief Privacy Officer.

Barry Tipping
Solicitor, Legal Services

Beverly Penjueli
Manager, Legal Services

RELEASED UNDER THE OFFICIAL INFORMATION ACT

FORM A - PRIVACY IMPACT ASSESSMENT FORM – Microsoft AZURE and Office 365 (O365)

"Personal information" held by Te Puni Kōkiri must be protected and dealt with in accordance with the Privacy Act 1993. "Personal information" is defined in the Privacy Act as *"information about an identifiable individual"*. As well as identifiers such as a person's name or email address, less obvious examples such as age or employment status fall within this definition if the way the information is recorded identifies the individual, accompanied by the person's name for example. In order to ensure that Personal Information in Te Puni Kōkiri is handled in accordance with the Privacy Act, could you please complete the following assessment for your area of work.

COLLECTION STAGE		
Privacy Act Requirements	**Questions**	**Answers**
Before you take steps to collect personal information, you must be sure that it is being collected for a purpose that is related to a lawful function of TPK and the personal information must be necessary for the purpose TPK wants to achieve.	What Personal Information is being Collected in your area? What is the purpose for which the Personal Information is being collected?	Microsoft AZURE is a cloud based storage platform. We will collect emails, data backups from some systems including our internal intranet which contains staff names & phone numbers. Microsoft Office 365 (O365) will be used to replace our current desktop version of Microsoft Office 2016 suite. It is an online service hosted by Microsoft. Staff will use this service to create/edit MS Office documents. N/A
Before you actually collect personal Information, the individual must be informed of the following: (Disclosure and Consent Process): • That the information is being recorded; • How it is being recorded (electronic and/or hard copy); • The purpose it is being collected for;	Have you obtained a Consent Form from Legal Services for the individual to sign before they give you their personal information?	N/A

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Document 6

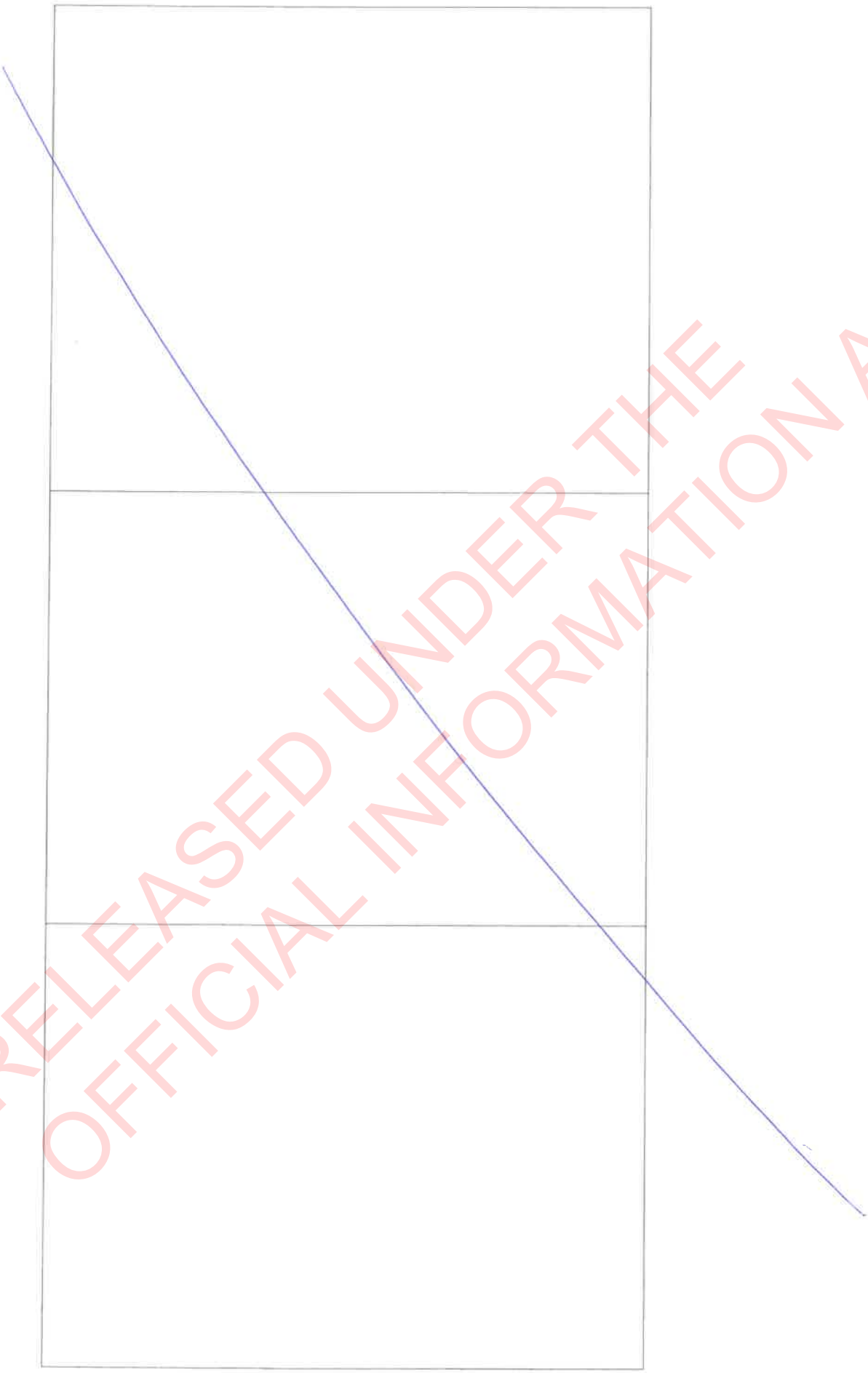
• Name and address of Agency collecting and the Agency that will hold the information. • Whether supplying the information is voluntary; • Consequences if request for information is declined; • Who will be able to access and use the information; • That the individual has the right to access and correct the information; and • The information will be destroyed once it is no longer needed.		
If TPK staff are collecting the personal information they must be made aware of the Personal Information Policy requirements and the Collection Processes above.	What steps have been taken to ensure that staff involved in handling this personal information been made aware of the Personal Information Policy requirements and the Collection Processes above.	TPK staff are aware of the Personal Information Policy, Privacy Act plus any related statutory or policy information.
If a third party is collecting the information for TPK then TPK must taken reasonable steps to ensure that they comply with the privacy Act too.	If a third party collecting is collecting the personal information for Te Puni Kōkiri, what steps been taken to: • require the third party to comply with the Privacy Act; and • require that the third party to confirm that it has privacy compliant processes in place for the collection, use, storage and disclosure of the information.	N/A
The Act requires Personal Information to be collected directly from the person themselves unless TPK has reasonable grounds to believe that the individual has authorised someone else to disclose their personal information to TPK.	Is the Personal Information being collected directly from the person themselves? If the Personal Information being collected from someone else, how will you ensure that the individual has authorised the disclosure? What steps have been taken to ensure that relevant staff been made aware of these requirements?	Yes, Information will be saved into our systems by TPK staff only. As per the Legal t&cs if information is being collected on behalf of someone else, the kaitiaki of that information will need to be made aware or give their consent.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Document 6

ACCESS AND STORAGE STAGE		
Privacy Act Requirements	**Question**	**Answer**
Personal Information is classified as "In Confidence" information under TPK's Classified Information Policy. So the following steps must then be taken in relation to the hard copy files and any databases on which the personal information is held: • Electronic files must be protected against illicit internal use or intrusion by external parties in accordance with Te Puni Kōkiri's Records Management Policy, Records Management Guide and Electronic Communication Policy. • Paper documents must be stored in accordance with Te Puni Kōkiri's Records Management Policy and Records Management Guide. • A list of authorised users will be approved by the responsible manager.	Where will the Personal Information be held? Who will have access to the Personal Information? How will the Personal Information be secure against loss or misuse. Has a list of "Authorised Users" been approved by the responsible manager. Has access to the files/database been restricted to those who "need to know". What steps have been taken to ensure that relevant staff been made aware of these requirements?	AZURE cloud service based in Australia Te Puni Kōkiri staff As per the AoG Cloud Assessment, "AZURE" does not access or use the suppliers' content without the customer's (Te Puni Kōkiri) consent, except as legally required. AZURE never uses the suppliers content or derives information from it for other purposes such as marketing or advertising". The A0G Cloud Risk Assessment once complete, will be approved by Michelle Hippolite – CE. Yes, The TPK Technical Information Architect will maintain and ensure connection to cloud services and storage access of data is secure at all times. Azure is only a storage platform and O365 a tool to create documents. There will be system and user restrictions in place as per current system restrictions Azure and O365 do not have any control over restricted access. Access is on a need to know basis and by TPK staff only. N/A

RELEASED UNDER THE OFFICIAL INFORMATION ACT



RELEASED UNDER THE OFFICIAL INFORMATION ACT

"Unique Identifiers" can be used to protect the names of individuals and remove the "privacy" implications. Recording information alongside a reference number as a unique identifier rather than a name might make the individual unidentifiable for example. Care should be taken about adopting a unique identifier unless necessary to carry out the purpose efficiently. An identifier assigned by another Agency *(such as an IRD number) should not be used. Using alternative references such as "the client" might make the individual unidentifiable.	Will unique identifiers be assigned to personal information? Why is this being done and what is the "unique identifier" system that is being proposed?	N/A. N / A.
The Act requires that: • Personal Information be kept up to date and accurate; and • individuals be able to access and correct personal information TPK holds about them. So processes need to be in place to allow access and changes to Personal Information.	What processes have been put in place to ensure that: a. Personal information held is accurate? b. Individuals are able to access their information and request changes? and c. only authorised changes are made to the information? What steps have been taken to ensure that relevant staff been made aware of this requirement?	a. It will be the responsibility of the Kaitono giving their personal information and / or those who have been approved to act on their behalf to provide accurate personal information. b. All staff will be able to access and edit (or request an edit) to their personal information in emails at any point c. Azure is only a storage platform and O365 a tool to create documents. There will be system and user restrictions in place as per current system restrictions Azure and O365 do not have any control over restricted access.

USE STAGE		
Privacy Act Requirements	**Question**	**Answer**

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Document 6

If the Personal Information is to be used for another purpose (i.e. not the purpose for which it was collected) then the consent of the individual must be obtained: a. the responsible manager must approve the individual being approached for the new purpose; and b. this new consent must be in writing and signed by the individual.	What steps have been taken to ensure that the consent of the individual is obtained before Personal Information is used for another purpose? What steps have been taken to ensure that relevant staff been made aware of this requirement?	N/A N/A
If you are electronically transmitting any personal information then you must: a. Double check that the email address that you are sending the information to is correct; b. Add the following statement to the bottom of your email: *"Te Puni Kōkiri is the originating government agency for this email. This email contains personal information which can only be used or disclosed in accordance with the Privacy Act. If you are the intended recipient then note that this information is disclosed "In-Confidence" and cannot be used for any purpose other than that which Te Puni Kōkiri has disclosed it to you. If you are not the intended recipient of this information please delete the email from your records and notify the sender by return email that you have received the information in error."*	What steps have been taken to ensure that relevant staff been made aware of this requirement?	All staff are informed of the risks around privacy breaches at Induction and via the TPK Privacy policy. Regular privacy reminders are sent out to all staff with increased comms on Privacy week. Azure is a storage platform only and O365 a tool to create documents. Privacy act requirements stated in the left column should be addressed by staff when transmitting personal information.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Document 6

c. If you are transmitting Personal Information in paper form, then you must: a. post the information in single sealed envelope with *"Private - To Be Opened By Addressee Only"* clearly written on the front of the envelope; and b. include a return address on the envelope in case delivery is unsuccessful.		

DISPOSAL STAGE		
Question	**Answer**	**Action Required:**
Personal information needs to be destroyed once it is no longer required for the authorised purposes. Disposal will need to be done in compliance with TPK's Records management Policy. You will need to consider: a. How long will the information be required for? b. What steps will need to be taken to initiate and complete the disposal process.	How long will the information be required for? What steps have been taken to ensure that Personal Information is destroyed once no longer necessary i.e. : a. Who will initiate the disposal process? b. Who will authorise the actual disposal? and c. Who confirms the information has been destroyed?	NĀ All staff emails contained in their deleted and sent item boxes are periodically purged by the system. Backup data stored on AZURE is replaced by the newer backup version each 24 hours.

Signed:

Greg Duncum Chief Information Officer 14/02/19

Approved

(M McBeath) 18 Feb 2019

Deputy Chief Executive
Chief Privacy Officer

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Document 6