

**Arrangement**  
between  
**Members of the Pacific Immigration Development**  
**Community**  
concerning  
**cooperation and capacity building**  
and the  
disclosure of information for immigration, border protection,  
law enforcement and public safety purposes

## Background

- A. The Pacific Immigration Development Community (“**PIDC**”) and its Constitution was recognised by its Member governments on [date]. The participants in this Arrangement are the official immigration agencies (“**Participants**”) of the following countries and territories: Australia, Cook Islands, Federated States of Micronesia, Fiji, French Polynesia, Kiribati, Republic of the Marshall Islands, Nauru, New Zealand, New Caledonia, Niue, Palau, Papua New Guinea, the Independent State of Samoa, Solomon Islands, Tonga, Tuvalu, and Vanuatu.
- B. The Participants enjoy a warm and cooperative relationship. The Participants share a common interest in the security, stability, and prosperity of the Pacific region.
- C. The Participants are also stewards of information, including personal information, which is subject to restrictions in terms of its use and disclosure (Annex One). They will protect that information, use it effectively, and exchange it appropriately so they can fulfil their respective immigration, border protection, law enforcement, and public safety responsibilities.

The Participants have accordingly reached the following understanding.

## Purpose and context

1. The purpose of this Arrangement is to support the Participants to share information to:
  - a. comply with their domestic and international legal obligations;
  - b. fulfil their respective immigration, border protection, law enforcement, and public safety responsibilities; and
  - c. combat regional risks and security issues including: human trafficking; smuggling of people, wildlife, arms, drugs and other illicit goods; transnational crime; money laundering and other financial crime; cyber-crime; environmental crime including illegal logging and fishing; organised crime; counter terrorism; corruption; immigration fraud; and other criminal activity.
2. The Participants work together in the context of their:
  - a. domestic engagement with other law enforcement and border agencies (such as Police, Customs, Health and Biosecurity agencies); and
  - b. international engagement with partners such as: the Pacific Transnational Crime Coordination Centre (“**PTCCC**”), Forum Fisheries Agency (“**FFA**”), Oceania Customs Organisation (“**OCO**”), the Pacific Islands Chiefs of Police (“**PICP**”), and the Pacific Islands Forum (“**PIF**”).
3. Each Participant will act consistently with:
  - a. any treaty obligations, such as the 1951 Convention Relating to the Status of Refugees (the “**Refugee Convention**”) and its 1967 Protocol relating to the Status of Refugees (the “**Refugee Protocol**”); the 1984 Convention against Torture and other Cruel, Inhuman or Degrading Treatment or Punishment (the “**CAT**”); the 1966 International Covenant on Civil and Political Rights (the “**ICCPR**”); the 2000 United Nations Convention Against Transnational Organised Crime (“**UNTOC**”); and the 2003 United Nations Convention Against Corruption (“**UNCAC**”);
  - b. its domestic laws implementing those treaty obligations; and
  - c. its domestic laws, including in particular its laws relating to the protection of sensitive information (sensitive information includes an individual’s criminal history, biometric information, financial information, health information, and any information about a minor).
4. This Arrangement reflects the Participants’ mutual interest to build and ensure cooperation between them, and to appropriately disclose relevant information in accordance with their respective domestic legislation, regulations, policies, and international obligations. For the avoidance of doubt, nothing in this Arrangement creates any legal relationship or legally-enforceable obligation between the Participants.
5. Each Participant will ensure that its employees, contractors, and all other entities that act on its behalf and whose duties involve the exchange of information under this Arrangement comply with the requirements established by this Arrangement.

### **General cooperation principles**

6. The Participants may, by mutual arrangement and subject to their domestic legislation and policies:
  - a. share general information on immigration, border protection, law enforcement, and public safety;
  - b. collaborate on initiatives to strengthen the capacity of the Participants and the PIDC Secretariat (the “**Secretariat**”) (for e.g. through exchange of personnel, secondments, sponsorship of personnel to specific training programmes, and the development of training programmes for delivery);
  - c. collaborate to develop and implement law, policy, and processes concerning immigration, border protection, law enforcement, and public safety; and
  - d. hold periodic meetings to monitor progress in achieving the objectives of this Arrangement.

### **National Contact Points and National Administrators**

7. The Participants will ensure that they maintain dedicated immigration National Contact Points (“**NCPs**”) (for day-to-day activity) and National Administrator (“**NAs**”) (for oversight and responsibility) for cooperation under this Arrangement. Each Participant will provide the Secretariat with updated contact details for their NCPs and NAs.

### **General rules for disclosing information (to a Participant or the Secretariat)**

#### *What Information may be disclosed*

8. The Participants may disclose the following information should the relevant domestic legislation allow for it (“**Information**”):
  - a. airline passenger and crew lists;
  - b. craft movements (which may include passenger and crew lists);
  - c. past travel movements of specified people;
  - d. previous convictions of specified people;
  - e. general history of specified people (which may include associates and networks);
  - f. modus operandi of specified people;
  - g. known currency and other financial transactions of relevant interest, including involvement in money laundering;
  - h. details of communications interceptions;
  - i. personal identification details (which may include photographs, biometric information, distinguishing features, and details of identity or travel documents);
  - j. names and details of immigration personnel and transport personnel;
  - k. details of known or suspected involvement of people in illicit activities;
  - l. details of any visa held by a person;
  - m. general non-personal information, including:
    - i.) the disclosure of technical, operational and other information;
    - ii.) the sharing of best practices regarding technical and operational matters;

- iii.) the disclosure of knowledge and expertise, legislative and regulatory documents and relevant scientific and technical information;
- iv.) the coordination of joint operations within their respective territories, in the frame of national joint operations or international joint operations; and
- v.) working cooperatively through the PIDC and the Secretariat on matters of common interest.

#### *When Information may be disclosed*

9. A Participant may disclose Information if:
- a. the disclosure is permitted by domestic legislation and any relevant policies;
  - b. it is satisfied that the Information relates to a suspected violation of its own law or the law of a receiving Participant; or
  - c. it is satisfied that the disclosure of Information is justified to help prevent, identify, or respond to violations of its law or the law of a receiving Participant; or
  - d. the subject of the Information consents to its disclosure; or
  - e. the disclosure is otherwise authorised or required by law.
10. A Participant may disclose Information with or without a request from another Participant or the Secretariat.

#### *To whom Information may be disclosed: Participants and the Secretariat*

- 10A. Participants may disclose Information to each other, the Secretariat, or both.

#### *Restrictions on disclosure: legal reasons*

11. A Participant may determine that disclosure, use, or further disclosure of certain Information would be inconsistent with its domestic laws or its international legal obligations (including under the Refugee Convention, the Refugee Protocol, the CAT, and the ICCPR). If so, the Participant may:
- a. refuse to disclose the Information; or
  - b. offer to provide all or part of the Information on specified terms and conditions.

#### *Restrictions on disclosure: policy and operational reasons*

12. A Participant may determine that disclosure, use, or further disclosure of certain Information would be detrimental to its operations, national sovereignty, national security, public policy, or other important national interest. If so, the Participant may:
- a. refuse to disclose the Information; or
  - b. offer to provide all or part of the Information on specified terms and conditions.

#### **How information may be disclosed to a Participant or the Secretariat**

#### *Secure disclosure*

13. The Participants intend to disclose Information by the most secure means necessary and practically available in each case. Means of disclosure will depend upon, amongst other things:
- a. physical and electronic security facilities available to each Participant;
  - b. the urgency and context for the disclosure; and
  - c. the sensitivity of the Information disclosed (sensitive information includes an individual's criminal history, biometric information, financial information, health information, and any information about a minor).
- 13A. The Participants intend to disclose Information in writing, unless doing so would be inappropriate considering:
- a. the urgency and context for the disclosure; and
  - b. the sensitivity of the Information disclosed.
14. In cases of particular sensitivity (for e.g. relating to ongoing investigations), Participants will consider using or developing virtual workspaces, encryption, or other means of disclosure.

#### *Disclosure through agents*

15. Where domestic legislation and policies allow, the Participants may disclose information through trusted agents or intermediaries (for e.g. the Secretariat, PTCCC, and diplomatic channels). Such disclosure may be by way of agents' and intermediaries' secure communication channels.

#### **How Information may be used by Participants**

16. A Participant may use Information disclosed to it for any purpose in para [1] of this Arrangement, unless:
- a. a particular caveat provides otherwise; or
  - b. the Information is disclosed under a particular annex to this Arrangement that provides otherwise.
17. A Participant may only use Information disclosed to it for any other purpose with the consent of the providing Participant and where the domestic laws permit it.

#### **Confidentiality and use of Information**

- 17A. The Participants undertake not to use or further disclose the Information provided under this Arrangement except:
- (a) in accordance with this Arrangement; or
  - (b) otherwise as required or authorised by law.

#### **How Information may be used by the Secretariat**

- 17B. The Secretariat may use Information disclosed to it to assist Participants to comply with or fulfil any purpose in para [1] of this Arrangement, unless:

- a. a particular caveat provides otherwise; or
- b. the Information is disclosed under a particular annex to this Arrangement that provides otherwise.

17C. Without limiting para [17B], the Secretariat may use Information consistent with

- a. this Arrangement; and
- b. general policy statements and priorities set by the PIDC Board.

**Further disclosure of Information by Participants and the Secretariat (outside the PIDC membership)**

18. Unless para [18A] applies, a Participant or the Secretariat may further disclose any Information disclosed to it to:

- a. any other domestic agency, body, or person for any purpose in para [1] of this Arrangement; or
- b. any international organisation, for any purpose in para [1] of this Arrangement.

18A. Neither a Participant nor the Secretariat may further disclose Information if:

- a. a particular caveat provides otherwise;
- b. the Information is disclosed under a particular annex to this Arrangement that provides otherwise;
- c. further disclosure by the Secretariat would be contrary to policy statements and Instructions from the PIDC Board;
- d. the Participant determines that its further disclosure would be inconsistent with its domestic laws or with international legal obligations (including under the Refugee Convention, the Refugee Protocol, the CAT, and the ICCPR); or
- e. the Participant determines that its further disclosure would be detrimental to its operations, national sovereignty, national security, public policy, or other important national interest.

19. Participants and the Secretariat may further disclose Information disclosed to it for any other purpose with the consent of the providing Participant or the Secretariat (unless, in the case of the Secretariat, such further disclosure would be contrary to policy statements and Instructions from the PIDC Board).

19A. The Participants and the Secretariat will seek to ensure that any agency, body, person, or international organisation to which it further discloses Information applies the same level of protection to the Information as under this Arrangement and limits disclosure in accordance with this Arrangement.

**Storage, deletion, and audit of Information**

20. The Participants and the Secretariat intend to store Information disclosed, further disclosed, and received under this Arrangement by the most secure means necessary and practically available in each case. Means of storage will depend upon, amongst other things:
- a. physical and electronic security facilities available to each Participant and the Secretariat;
  - b. the urgency and context for the disclosure; and
  - c. the sensitivity of the Information disclosed.
21. The Participants and the Secretariat intend to delete Information when it is no longer useful for the purposes in para [1] of this Arrangement.
- a. The Participants will make deletion decisions in accordance with their domestic legislation; and
  - b. The Secretariat will make deletion decision in accordance with guidance from Participants.

### **Audit**

22. The Participants and the Secretariat will ensure that, as far as possible, they can track and audit their disclosure, further disclosure, and use of Information under this Arrangement. Tracking and auditing must include:
- a. the Information disclosed or further disclosed;
  - b. the agency, body, or person to whom it was disclosed;
  - c. the conditions subject to which it was disclosed; and
  - d. when the Information was disclosed.
- 22A. A Participant may request another Participant or the Secretariat to provide such tracking and auditing information if the need arises. The Secretariat may ask a Participant to provide such tracking and auditing if the need arises. If a Participant or the Secretariat receives a request for tracking and auditing information it will provide reasonable assistance to the requestor.

### **Disclosure in particular cases**

#### *Annexes*

23. The Participants may if required, make annexes to this Arrangement to govern specific classes of use, disclosure, or further disclosure.
24. Annexes may set out any additional details about the Information that may be exchanged, methods of sharing, storage and retention, any operational procedures or additional security mechanisms, or other safeguards to be followed. This may include (but is not limited to):
- a. types of Information to be disclosed (such as profile rules, code, techniques, and procedures relating to data analysis);
  - b. scenarios for Information disclosure (such as support for particular operations);



- c. criteria for Information disclosure (such as matters of particular concern to border security);
- d. modes of Information disclosure (such as automated or high-volume disclosures); and
- e. arrangements for the tracking and auditing of any disclosure, use and further disclosure of Information disclosed under this Arrangement.

25. Annexes may provide that certain Information disclosed under the terms of this Arrangement are subject to certain conditions.

26. Without limiting the generality of para [25], Annexes may set out:

- a. that the Participant receiving Information will not disclose it to any other agency, body, or person; or
- b. the other agencies, bodies, or persons to which the Participant receiving Information may disclose any of it, and the extent to which and conditions subject to which the Participant may do so.

27. Annexes remain subject to this Arrangement and are intended to be consistent with the provisions of this Arrangement and the Participants' respective domestic laws, international obligations, regulations, and policies.

#### **Differences**

28. The Participants accept that any differences arising over the interpretation or implementation of this Arrangement, including its Annexes, will be amicably settled in consultation and negotiation between the Participants.

#### **Commencement, Duration and Termination**

29. This Arrangement will come into effect on the date that the PIDC Member signs and becomes a Participant to the Arrangement.

30. This Arrangement is intended to remain in effect for an unlimited duration. It may be terminated at any time if two-thirds of Participants give notification of termination to all other Participants in writing. Such termination will take effect ninety (90) calendar days from the date of the notification unless the Participants mutually consent to a shorter period of time.

- (a) where this Arrangement is terminated under paragraph 30, the Annexes are also terminated;
- (b) a Participant may withdraw from this Arrangement at any time by notification to all other Participants in writing. Such withdrawal will take effect ninety (90) calendar days from the date of the notification unless the Participants mutually consent to a shorter period of time; and
- (c) where a Participant withdraws from this Participant under paragraph 30(b), that Participant also withdraws from the Annexes.

31. Ongoing transactions at the time of withdrawal or termination will nonetheless be completed in accordance with the provisions of this Arrangement.

DRAFT

## Amendment

32. The Participants may mutually determine to amend or modify this Arrangement and any such amendment or modification will be mutually decided in writing and distributed to all Participants via the Secretariat.

33. An amendment or modification to this Arrangement will come into effect on the date the amended or modified Arrangement is signed by two-thirds of the Participants.

34. Notwithstanding termination of this Arrangement, the provisions of paragraph 16, 17, and 17A will continue to apply to Information received pursuant to this Arrangement.

## Review

35. The Participants will review this Arrangement annually at the PIDC Regular Annual Meeting.

SIGNED at )  
for and on behalf of )  
[agency] by )  
)

[insert name]

Authorised Delegate  
on

\_\_\_\_\_  
signature

\_\_\_\_\_  
date

[repeat signatories]

---

[1] This list is based on s 306(1) of the Immigration Act 2009 (NZ).  
[2] Section 305(7)

## INFORMATION SECURITY CLASSIFICATION

### Purpose

The purpose of this document is to recommend to the PIDC guidelines for Information Security Classification. These guidelines are recommended to PIDC Members to assist in improving information management through the ISWG contact point, and if information is required to be shared with other Law Enforcement Agencies.

### Acknowledgements

This paper is largely based on the work of Andrew Walker (New Zealand Customs Service) for the Pacific Islands Forum Secretariat (PIFS) in 2014. We would like to thank Andrew and PIFS for sharing their work, and enabling the PIDC to develop a similar Information Security Classification.

### Background

In recognition of the growing threat of irregular migration and organised crime to the Pacific region, limited resources available to Pacific Islands Immigration administrations, and the need for Pacific Islands to strengthen their law enforcement and border management capacity to advance national and regional strategic objectives, PIDC Members in their 2016 Regular Annual Meeting:

- i. *Noted the value of using immigration data to manage and monitor the movement of people;*
- ii. *Agreed on the importance of information sharing to help monitor people movement, risks and opportunities; and*
- iii. *Tasked the Secretariat to consider surveying Members or establishing a Working Group to identify information sharing capabilities and requirements, with the purpose of supporting the establishment of information sharing MoUs.*

The PIDC Information Sharing Working Group (ISWG) was developed with a membership of Australia, New Zealand, Tuvalu, Palau, Samoa, Vanuatu, and Fiji. The ISWG are undertaking four key tasks initially to enable and increase the level of information sharing for immigration risk within the region. These include developing an MoU for information sharing; developing contact points for effective and trusted information sharing; developing a platform for information sharing; and endorsing a classification system within which PIDC Members can classify information to share.

- And the Pacific Trans-national Crime Network (PTCN) brought together by the Pacific Transnational Crime Coordination Centre (PTCCC)

## Need to Know – Need to Share

A principle for limiting the likelihood that information or intelligence is shared beyond its intended audience is the “need to know” principle. This means that information is only shared with officers who have a proven need to know of it.

The beauty of this principle is its simplicity. All that is required is a level of common sense and commitment to be effective. The problem with this principle is that in order for intelligence to be effective it has to be used and for that to happen it often needs to be shared.

Information and intelligence sharing is recognised as a vital tool to enable law enforcement agencies to effectively target and disrupt organised crime. The wider the dissemination the greater the risk of compromise, however abiding by appropriate methods of storage and transmission for classified information can minimise this risk.

Within the PIDC membership, there will be trusted and accredited contact points with whom you can share information. Firstly, we encourage the sharing of information through the PIDC Secretariat, who can distribute the information to those who need to know. In some cases, you may deem the information important for wider dissemination to relevant law enforcement agencies. In this case, please provide the information to the PTCCC in accordance with relevant domestic legislation, regulations, policies, and international obligations.

Information and intelligence needs to be assessed on a case by case basis in order to establish the appropriate balance between “need to know” and “need to share”.

In all cases where intelligence and information which originated from outside your organisation is to be disseminated to a third organisation, the originating agency **must** be consulted before dissemination is undertaken.

## Classifications

The classifications recommended appear in the New Zealand classification guidelines. They will be familiar to Pacific Island Countries that have strong ties with New Zealand.

The recommended classifications for information are:

**IN CONFIDENCE** – When disclosure would prejudice law and order, impede government business, or affect the privacy of citizens.

This classification is used where improper release of the information could prejudice law and order, impede government business, or affect citizens privacy.

Examples of information which are classified in confidence by Immigration New Zealand:

- Visa application details

Reason: The release of this information could compromise the privacy of individuals

- Investigation notes

Reason: The release of this information could prejudice law and order

**RESTRICTED // FOR OFFICIAL USE ONLY** – When disclosure would adversely affect national interests, damage government interests, or endanger citizens.

This classification is used where improper release of the information could adversely affect the national interest. Significantly hinder the operational effectiveness of government. Endanger the safety of any person or adversely affect internal stability, and adversely affect economic wellbeing.

Examples of information which are classified restricted by Immigration New Zealand:

- List of countries whose nationals are screened for associations with war crimes
- List of countries whose nationals undergo a security check

Reason: The release of these lists could adversely affect New Zealand government's diplomatic relationships.

## Storage

Information should be stored in a manner commensurate with the damage that would be caused by disclosure of the information beyond its intended audience. Measures taken can range from keeping documents within a government building with access control (a lock on the door), through to dedicated storage containers (safes).

Electronic storage should also be appropriate for the level of classification that a document is given. Suggestions and requirements for the storage and transmission of both physical and electronic material are given in the tables within Appendix 1.

## Transmission

Information should be transmitted in a manner commensurate with the damage that would result through inadvertent disclosure beyond its intended audience. Secure networks are to be used to transmit classified information. Personal email accounts (for e.g. Hotmail, gmail etc) are not to be used to transmit classified information.

The ISWG has been tasked with identifying a secure channel of communication to allow PIDC Members to freely and securely share information. In the interim regional networks such as the PTCN/PTCCC offer secure on-line portals that should be considered for the transmission of classified information when appropriate.

## Classification of Information

Information is assessed on its creation by the originator or creator of that information (if they are within a government organisation), or by the person within a government organisation who will make use of the information. This person is known as the originator.

If the originator assess that there is a risk in the disclosure of the information, then an appropriate information classification should be used. It is the responsibility of the originator to set an appropriate classification and care should be taken not to over classify. Information that does not require protection should remain unclassified.

If classified information is received it must keep the level of classification that it carries when received and afforded the appropriate precautions with regards to storage and transmission. Changes to the classification of information can only occur with the permission of the originator who set the initial level of classification.

Classification	When it is used	Storage of Information	Transmission
<b>IN CONFIDENCE</b> – Prejudice law and order, impede government business, or affect citizen privacy.	This classification is used where improper release of the information could prejudice law and order, impede government business, or affect citizens privacy.	<p>Paper: Documents can be stored using normal building security so long as it keeps the public out of administration areas.</p> <p>Electronic: Electronic files should be protected from illicit external use or intrusion through two or more of the following:</p> <ul style="list-style-type: none"> <li>• User challenge and authentication.</li> <li>• Firewalls and intrusion detection systems.</li> <li>• Server authentication.</li> <li>• OS specific / application specific security measures.</li> </ul>	<p>Paper: May be posted in a single sealed envelope. May be carried by ordinary postal or commercial courier firms provided the envelope or package is sealed. The envelope must clearly show a return address in case delivery is unsuccessful. A PO box would suffice.</p> <p>Electronic: Information must be marked IN CONFIDENCE. In Confidence data can be transmitted across external or public networks without being encrypted. All IN CONFIDENCE information is to clearly identify the originating government agency.</p>
<b>RESTRICTED</b> – Adversely affect national interests, damage government interests, or endangers the safety of any person.	This classification is used where improper release of the information could adversely affect the national interest. Significantly hinder the operational effectiveness of government. Adversely affect internal stability, or adversely affect economic wellbeing. It is also used when improper release would endanger the safety of any person.	<p>Paper: Restricted documents should be stored in a secure container (for e.g. a locked cabinet) within a secure building.</p> <p>Electronic: Electronic files MUST be protected from illicit external use or intrusion through two or more of the following:</p> <ul style="list-style-type: none"> <li>• User challenge and authentication.</li> <li>• Firewalls and intrusion detection systems.</li> <li>• Server authentication</li> </ul> <p>OS specific / application specific security measures.</p>	<p>Paper: Documents when posted must be double enveloped. May be carried by ordinary postal or commercial courier firms provided the envelope or package is sealed and the word RESTRICTED is not visible. The outer envelope must clearly show a return address in case delivery is unsuccessful. A PO box would suffice. The outer envelope should be addressed to an individual by name and title.</p> <p>RESTRICTED mail for or from overseas should be carried by diplomatic airfreight.</p> <p>Electronic: Information must be marked RESTRICTED. All RESTRICTED information transmitted across public networks should be encrypted. Please contact PTCCC for this service.</p>