Owner:	MPI Organisational Policy	24 March 2016
Chief Security and Privacy Officer	**Privacy Management**	

Overview

Purpose

The purpose of this policy is to ensure that individuals can have trust and confidence in the way that MPI manages their personal information, and to set out MPI's responsibilities:

- under the Privacy Act in relation to personal information; and
- with respect to inquiries and investigations by the Privacy Commissioner under the Privacy Act and generally.

KEY ACCOUNTABILITIES

- The Director-General is accountable for compliance with the Privacy Act and has delegated authority to various senior managers within MPI. Authority is delegated to make decisions to release personal information, in what manner and any charges.
- MPI's Chief Privacy Officer is currently the Chief Security and Privacy Officer supported by the Senior Advisor Privacy as Deputy Privacy Officer.

Background

The Privacy Act applies to all personal information held by MPI about an identifiable living individual. Personal information means any information that identifies someone. The 12 information privacy principles in the Privacy Act cover all information management activities; including the collection, storage and security, use , disclosure, access to and correction of personal information. In addition, the public register privacy principles in the Act cover personal information in certain public registers administered by MPI.

The Privacy Act also applies to requests from individuals for access to, and correction of, their personal information, even if the Privacy Act is not mentioned in the request. However, the Privacy Act does not apply to requests:

1. from individuals for personal information about other people; or
2. from organisations. These are usually considered under the Official Information Act.

Although any MPI staff member may assist with a Privacy Act request, personal information may only be released after approval by those with a delegated authority.

Scope

This Policy:

- provides guidance, in conjunction with the Procedures and Guidelines to MPI staff about:
    1. proactive consideration of privacy considerations as part of the work of MPI;

2. responding to personal information requests; including decisions to release or charge for personal information;
3. complaints to, and inquiries and investigations by, the Privacy Commissioner; and
4. adherence to the information privacy principles.

- applies to all personal information held by MPI, including information held at an overseas post which has been transferred from NZ by MPI or another agency.

Note: All sections of this policy and its associated guidelines and procedures contribute to the policy position.

REQUIREMENTS:

Shared Responsibilities

All decisions on requests for personal information are to be managed in accordance with the Privacy Act.

Where an individual requests the release or correction of information about himself or herself the Privacy Act applies to the request.

Currently, the Chief Security and Privacy Officer is MPI's Chief Privacy Officer supported by the Senior Advisor Privacy as Deputy Privacy Officer.

MPI will:

- Ensure the information privacy principles and public register privacy principles are adhered to;
- Collect personal information only that is necessary for a lawful purpose and do so fairly;
- Collect it from the individual directly unless an exception applies;
- When appropriate, tell individuals that personal information is being collected and what we are doing with it;
- Hold personal information securely with reasonable safeguards against loss or unauthorised use or release;
- Provide access for individuals to information about themselves in accordance with the Act and release the person's information to them in an appropriate manner, or refuse when certain circumstances allow (those prescribed in the Act);
- Comply with statutory timeframes prescribed in the Act;
- Have processes for the correction of personal information;
- Ensure the accuracy of personal information before we use it (to the extent reasonable given the purpose of use);
- Hold personal information for no longer than necessary and dispose of personal information securely;
- Not use or disclose personal information for other purposes unless an exception applies;

- Adopt proactive measures, such as privacy impact assessments (PIA), to establish how privacy risks identified in proposed systems can be managed;
- Adopt proactive incident management processes and procedures to mitigate or eliminate privacy breach risks;
- Design information systems with privacy in mind;
- Act in accordance with the MPI Privacy Procedures; and
- Not require payment of any charge for an information privacy request other than as authorised by the Act.
- Adopt a system for gaining assurance that it is complying with this policy

Privacy Commissioner Inquiries and Investigations

MPI is required to co-operate with an inquiry or investigation by the Privacy Commissioner. All Privacy Commissioner inquiries and investigations must be logged with the Ministerial & Business Support Group.

All responses to the Privacy Commissioner:

1. must be cleared by the Chief Privacy Officer or Deputy Privacy Officer prior to signature; and

2. may be signed only by the Director-General, a relevant Deputy Director-General or Chief Operations Officer, the Chief Privacy Officer or the Deputy Privacy Officer.

Where a deadline for response is not included in correspondence with the Privacy Commissioner, 20 working days is taken as a default due date. Where a response is dependent on input from the Privacy Commissioner or a complainant, it is important to keep the Ministerial Coordinator up to date on any implications of the deadline.

Any correspondence from the Privacy Commissioner concerning a complaint made to them by a person who has requested information under the Privacy Act must be referred to the Ministerial & Business Support Group.

Government Chief Privacy Officer

The Government Chief Privacy Officer (**GCPO**) has issued core expectations that represent good practice for privacy management and governance. MPI will work with the GCPO to develop capability and implement appropriate improvements consistent with MPI's privacy maturity assessment.

Privacy Breaches and Voluntary Reporting

A privacy breach results from unauthorised access to or collection, use or disclosure of, personal information.

If a staff member becomes aware that a privacy breach has occurred, the Information Security Framework process should be followed and the Chief Privacy Officer and/or Deputy Privacy Officer should be informed as soon as possible. The process can be found at:
http://kotahi.mpi.govt.nz/do/security-and-privacy-mpi/privacy

If MPI becomes aware that a privacy breach has occurred, MPI will:

- contain the breach and perform an initial investigation;
- evaluate the risks;
- consider or undertake notification of affected individuals and the Privacy Commissioner; and
- develop and put in place future prevention strategies.

Privacy Impact Assessment Reports

A Privacy Impact Assessment Report (PIA) is a systematic process for evaluating a proposal in terms of its impact on privacy.

MPI has developed PIA templates and guidance material identifying what projects need to complete. These should be used when new systems or changes to systems that process personal information are proposed.

BREACHES OF POLICY

Failure to comply with this Policy may amount to a breach of the Code of Conduct for MPI employees.

LEGISLATION

Criminal Disclosure Act 2008

Official Information Act 1982

Privacy Act 1993

STATE SECTOR GUIDANCE

Links that offer further guidance include:

Government Chief Information Officer, see "Privacy and Security" Guidance and Resources www.ict.govt.nz

Chapter 8 of the Cabinet Office Manual www.cabinetmanual.cabinetoffice.govt.nz/8

Office of the Privacy Commissioner www.privacy.org.nz/

Data Safety Toolkit www.privacy.org.nz/news-and-publications/guidance-notes/data-safety-toolkit/#one