Ministerial Policy Statement

The management of information obtained by GCSB and NZSIS, including retention and disposal of that information

Summary

It is necessary for employees of the Government Communications Security Bureau (GCSB) and New Zealand Security Intelligence Service (NZSIS) to collect information, including personal information, in the course of performing those agencies' statutory functions. This ministerial policy statement (MPS) provides guidance for employees on the management of information collected by GCSB and NZSIS. It does not apply to common corporate service public records.

In making decisions related to information management, employees must have regard to the following principles: necessity and relevance, shared responsibility, management of access, security of information and oversight. This ministerial policy statement also specifies certain additional matters to be included in internal policy and procedures.

Definitions

The Act *means the Intelligence and Security Act 2017.*

Employee*, in relation to an intelligence and security agency, means a person employed in any capacity in that agency.*

Disposal *is defined as in the Public Records Act 2005 and means the transfer of control of a record or the sale, alteration, destruction, or discharge of a record.*

GCSB *means the Government Communications Security Bureau.*

Information *means data and information collected by GCSB and NZSIS in the performance of statutory functions, through any method, including warranted and lawful unwarranted collection methods.*

Information management / Management of information *means the processes of recording, storing, reviewing, disposing of, and sharing information for the purpose of performing one or more statutory functions of GCSB and NZSIS.*

Information privacy principles *are the information privacy principles contained in Part 2 of the Privacy Act 1993.*

NZSIS *means the New Zealand Security Intelligence Service.*

Personal information *means information about an identifiable individual.*

Public record *is defined as in the Public Records Act 2005 and means a record or class of records, in any form, in whole or in part, created or received by a public office in the conduct of its affairs. Public records are subject to specified retention and disposal requirements under the Public Records Act.*

Record *is defined as in the Public Records Act 2005, and means information, whether in its original form or otherwise, including (without limitation) a document, a signature, a seal, text, images, sound, speech, or data compiled, recorded, or stored, as the case may be, – (a) in written form on any material; or (b) on film, negative, tape or other medium so as to be capable of being reproduced; or (c) by means of any recording device or process, computer, or other electronic device or process.*

Restricted information *is defined as in section 135 of the Act, and means information relating to the secrecy requirements of Inland Revenue, national student numbers, adoptions, and driver licensing photographs.*

Purpose

1. This MPS is issued by the Minister Responsible for the GCSB and the Minister in Charge of the NZSIS pursuant to section 206(h) of the Act.
2. The purpose of the MPS is to provide guidance to GCSB and NZSIS on the management of information by those agencies, including the retention and disposal of that information. The MPS comprises the Minister's expectations for how GCSB and NZSIS should properly perform their functions and establishes a framework for good decision-making and best practice conduct.
3. This MPS supports GCSB and NZSIS to fulfill information management obligations contained in the existing legal framework for the management of personal information (Privacy Act 1993), official information (Official Information Act 1982), and public records (Public Records Act 2005), and the specific obligations imposed by the Act in relation to certain categories of information. GCSB and NZSIS are required to meet their obligations under this legislation and any associated mandatory standards (for example, the Information and records management standard issued by the Chief Archivist), as well as the New Zealand Protective Security Requirements, New Zealand Government Security Classification System, and New Zealand Information Security Manual.
4. MPSs are also relevant to oversight of GCSB and NZSIS by the Inspector-General of Intelligence and Security in the exercise of her propriety jurisdiction (the Act requires the

Inspector-General of Intelligence and Security to take account of any relevant MPS and the extent to which an agency has had regard to it when conducting any inquiry or review).

5. Every employee of GCSB and NZSIS must have regard to this MPS. Employees should be able to explain how they had regard to the MPS. This might amount to an explanation of their consideration of any relevant internal policy or procedures that reflect the MPS. The Directors-General are responsible for ensuring the MPS is reflected in their agency's internal policies and procedures. If any action or decision is taken that is inconsistent with the MPS, employees must be able to explain why the action was taken and how they had regard to the MPS.

Scope

6. This MPS applies to all information obtained, created, collected and/or managed by GCSB and NZSIS in the course of exercising their statutory functions. It includes information intercepted, seized, copied or otherwise obtained under a warrant or authorisation (issued under Part 4 of the Act) or other lawful means that do not require a warrant (including but not limited to those methods specified in Parts 3 and 5 of the Act). Information may include video recordings and photographic images, as well as data obtained from electronic tracking.
7. This MPS applies to all records created and received by GCSB and NZSIS in the course of fulfilling all statutory functions, duties and responsibilities, to ensure appropriate storage, handling, retention and disposal of those records.
8. This MPS does not apply to records that fall under General Disposal Authority 6 (Common corporate service public records) and General Disposal Authority 7 (Facilitative, transitory, and/or short-term value records) issued by the Chief Archivist under the Public Records Act 2005. Those disposal authorities cover a generic class of records created through routine administrative and business functions which are common to most public service departments, for example human resources, finance, administration and records that have only short-term, transitory value in their immediate and minor facilitation of preparing a more complete public record. Personnel files of GCSB and NZSIS are subject to a separate disposal authority and are also outside the scope of this MPS.
9. Where information has been obtained through an information-sharing agreement with a foreign partner, this MPS should be read in conjunction with the MPS on *Cooperation with overseas public authorities*.

Context

10. GCSB's and NZSIS's objectives are set out in the Act. Both agencies contribute to:
    a) The protection of New Zealand's national security;
    b) The international relations and well-being of New Zealand; and
    c) The economic well-being of New Zealand.
11. GCSB and NZSIS do this through the performance of their statutory functions, which are:
    a) Intelligence collection and analysis;
    b) The provision of protective security services, advice and assistance;
    c) Cooperation with other public authorities to facilitate their functions; and
    d) Cooperation with other entities to respond to imminent threat

12. MPSs are an important component of the measures put in place by the Act to ensure the functions of GCSB and NZSIS are performed with propriety and in accordance with New Zealand law and all human rights obligations recognised by New Zealand law.

13. In order to perform any of their statutory functions, GCSB and NZSIS must be able to obtain and use a wide variety of information, including at times personal and restricted information. Effective management of this information through the entire lifecycle of collection, analysis, storage, protection, dissemination and disposal is therefore vital for the agencies' core business, as well as meeting legal obligations. Sound information management policies and practices are also important to minimize the intrusiveness of the agencies' information collection and storage.

Sources of information

14. The Act allows GCSB and NZSIS to lawfully collect information using a variety of methods, some of which may be covert and without the knowledge of any person(s) about which information has been collected:

    a) Part 4 of the Act provides for intelligence warrants, which allow GCSB and NZSIS to collect information using methods that would otherwise be illegal, such as conducting surveillance, intercepting private communications, searching places or things, and seizing communications.

    b) Part 5 of the Act provides for GCSB and NZSIS to request information held by other agencies, to have direct access to databases that store specific public sector information, to access specified categories of restricted information, and to obtain the business records of telecommunications network operators and financial service providers.

15. GCSB and NZSIS may also collect information through a variety of other lawful (and which do not require specific authority) means, such as by using human sources, from publicly available information, through surveillance in a public place, and through the provision of information assurance and cybersecurity services. The conduct of collecting information using these means is addressed in a number of related MPSs (see MPSs on *Surveillance in a public place*; *Information assurance and cybersecurity activities*; *Collecting information lawfully from persons without an intelligence warrant (HUMINT*; and *Obtaining and using publicly available information*).

16. GCSB and NZSIS may also obtain information through information-sharing agreements with foreign partners. This source of information is addressed through a separate MPS (see MPS on *Cooperation with overseas public authorities*).

Legal framework

17. As noted above GCSB and NZSIS have information management obligations under a number of pieces of legislation, as well as under additional mandatory government standards and requirements. The general requirements of government-wide legislation (such as the Public Records Act 2005) and specific requirements contained within the Act are complementary. This MPS outlines the various requirements and their application to GCSB and NZSIS.

18. At the general level GCSB and NZSIS have an obligation, as public service departments, to ensure that their information is managed effectively in a way that supports the performance of their statutory functions and enables them to meet their business needs, and supports

accountability requirements and the transparency expectations the public has of government. In addition, there are also specialist oversight requirements in place for GCSB and NZSIS due to the sensitive and at times intrusive nature of the powers and functions conferred on them in the Act.

19. Recognising this, section 17(d) of the Act requires GCSB and NZSIS to perform their functions in a manner that facilitates effective democratic oversight. Good information management and record keeping is fundamental to effective oversight: GCSB and NZSIS must know what information it has stored and where, who has accessed stored information and for what purpose, and be able to locate it, in order for it be accessed when lawfully requested (such as by the Inspector-General of Intelligence and Security, or via a Privacy Act or Official Information Act request).
20. Competing with a general drive for the retention and openness of government information, is the more specific need to effectively manage the range of sensitive information handled by GCSB and NZSIS and to protect the methods used to collect that information. This includes specific obligations imposed by the Act to ensure that certain types of information are not retained.

Public Records Act 2005

21. The Public Records Act 2005 supports the accountability of Government by ensuring that full and accurate records of the affairs of central government are created and maintained, and by providing for the preservation of, and public access to, records of long-term value.
22. Section 17 of the Public Records Act 2005 requires GCSB and NZSIS to create and maintain full and accurate records of its affairs in line with normal, prudent business practice. It also requires GCSB and NZSIS to maintain all public records in an accessible form until their disposal is authorised. Section 18 specifically forbids the disposal of public records unless authorised by the Chief Archivist or when required by another Act. In accordance with section 20 of the Public Records Act 2005, disposal may occur by transferring control, altering or destroying, selling or discharging the public record.
23. These requirements mean that GCSB and NZSIS must retain all information they receive or create in the conduct of their affairs, unless:
    - the disposal of that information is authorised by the Chief Archivist (either under a General Disposal Authority or an agency-specific disposal schedule approved by the Chief Archivist); or
    - the disposal is authorised or required by another piece of legislation (the agencies must destroy information they are legally required to destroy – for example the Act has specific obligations in terms of information collected under an authorisation that is not relevant information).
24. Agencies are not authorised to dispose of information that has long-term archival value as records of the activities of the government of the day. These records will show evidence of the agencies' functions, policies, decisions, procedures or operations. GCSB and NZSIS are required to transfer these records to Archives New Zealand after no longer than 25 years, unless there are reasons for deferring that transfer.

Privacy Act 1993

25. The Privacy Act 1993 promotes and protects individual privacy, by setting out the principles for how public sector agencies should collect, use, disclose and allow access to personal information (the information privacy principles).

26. GCSB and NZSIS will regularly be required to collect and hold personal information in the course of performing their statutory functions, and therefore the information privacy principles which apply to GCSB and NZSIS are of particular relevance in the management of that information. Due to the nature of some of the agencies' collection methods (including the need to collect information without the person knowing it), GCSB and NZSIS are exempt from principles 2, 3, and 4 (b). Due to the agencies' statutory functions, GCSB and NZSIS have specific exceptions that apply to principles 10 and 11. These exceptions relate to using and disclosing information that has been collected for one purpose for limited secondary purposes.

Official Information Act 1982

27. The Official Information Act 1982 (OIA) aims to increase the availability of official information (broadly, any information held by a government department) to New Zealanders to promote both the effective participation in government law and policy-making and the accountability of Ministers of the Crown and officials. The OIA protects official information to the extent consistent with certain public interest considerations, including the preservation of personal privacy.

28. GCSB and NZSIS have a general obligation under the OIA to make official information available when requested, unless there is a good reason for withholding it under sections 6 (conclusive reasons), 7 (special reasons), and 9 (other reasons). A national security classification is not in itself a justification for withholding information requested under the OIA: every request must be considered on its merits against these criteria. Section 10 (neither confirming nor denying the existence or non-existence of information) and section 18 (refusal of requests) provide additional responses to requests for information. In order to be able to respond to requests, GCSB and NZSIS must be aware of what information is held and be able to access it.

Intelligence and Security Act 2017

29. The Act contains a number of provisions relating specifically to information obtained and held by GCSB and NZSIS, which may modify obligations under the Public Records Act and Privacy Act. These include:

    a) The obligation to destroy as soon as practicable all information obtained under an urgent or very urgent authorisation if that authorisation is subsequently revoked (including by operation of law), unless section 104 applies (see below) [sections 76 and 81];

    b) The obligation to immediately destroy unauthorised information (information unintentionally obtained that is outside the scope of an authorisation or authorised activity), unless a warrant is obtained as soon as practicable or section 104 applies (see below) [section 102];

Example one:

Information about a New Zealander is obtained under a Type-2 warrant. It is not known that the person was a New Zealander when the warrant was sought. A Type-1 warrant should be sought or the information destroyed.

c) The obligation to destroy as soon as practicable information that is obtained within the scope of an authorised activity but is irrelevant to the performance of the agency's functions, unless retention is required by any other laws or court orders [section 103];

Example two:

Under the authority of an intelligence warrant private communications may be lawfully intercepted. Relevant information would include phone calls about a specific subject matter, while irrelevant information might include phone calls made as a result of calling the wrong number.

Example three:

Information that is seized from a computer under an authorisation that, following analysis, is identified as being of no intelligence value.

d) The ability to retain incidentally obtained information (whether obtained through an authorisation or other means), only for the purposes of disclosing that information to the New Zealand Police, New Zealand Defence Force, or other public authority in order to assist them to fulfil their own statutory functions related to serious crime, threat to life, threats to the security or defence of New Zealand or another country, or the death of any person outside the territorial jurisdiction of any country [section 104]; and

Example four:

Information about an armed robbery that is collected during an authorised interception of communications but is not relevant to the agency's investigation (and therefore not relevant to their statutory functions) may be retained but only in order to provide that information to the Police for the purpose of preventing a serious crime in New Zealand.

e) The obligation to destroy as soon as practicable all business records information obtained under a business records direction if the records are irrelevant to the performance of the agency's functions, unless retention is required by any other laws or court orders [section 152].

30. The Act also establishes a number of offences (which carry fines of up to $10,000, or imprisonment of up to two years and a fine of up to $10,000) relating to the unlawful use and disclosure of information held by GCSB and NZSIS:

    a) Unlawful use or disclosure of information: it is an offence to use or disclose to another person any information obtained during an authorised activity, other than for purposes of performing the person's functions, duties or powers or with the consent of the Minister [section 108];

    b) Unlawful disclosure of acquired information: it is an offence to knowingly disclose information known to have been acquired from an authorised activity, other than in the course of fulfilling statutory functions, duties and powers [section 109];

    c) Duty of confidentiality: unless authorised by the responsible Minister for an intelligence and security agency, persons must keep confidential all information that comes into their knowledge in the performance of their functions, duties and powers and must not make a record or disclose that information except for the purpose of carrying out their functions or duties. Failure to comply with this duty is an offence [section 219].

31. It is therefore important that GCSB and NZSIS have information management practices and procedures in place that protect information from being used in any manner that would constitute one or more of these offences, regardless of whether that is by current or former employees, or any other person.

Principles

32. The Directors-General of GCSB and NZSIS are responsible for the management and use of information obtained by the agencies in the course of performing their statutory functions. They must also ensure that they have in place policies and procedures that ensure such information is used effectively for those purposes and in compliance with the legal obligations discussed above. Where appropriate, legal advice will be sought.

33. The following principles constitute a framework for good practice and are to be taken into account by GCSB and NZSIS when developing internal information management policies and procedures. The management of information should be subject to ongoing review as to whether it continues to be consistent with these principles.

Necessity and relevance

34. The collection, access, use and retention of information by GCSB and NZSIS must be justified by a connection with the performance of a statutory function(s) of the agency. To meet this principle GCSB and NZSIS should, in the first instance, only collect information that is necessary to fulfill statutory function(s) and, as soon as practicable, assess collected information for relevance to the performance of a statutory function. Subject to legal requirements to retain information for longer, information should only be retained for as long as it is relevant to the performance of a statutory function.

35. From time to time the agencies will inevitably collect information that is not relevant to the performance of statutory functions, and that is explicitly recognised by the destruction provisions contained within the Act. GCSB and NZSIS must have guidelines in place to assist employees to determine whether information is relevant to the performance of statutory functions, and which specify the timeframes in which that determination must be completed. Assessments of relevance must, at a minimum determine whether the

information collected is required to support the performance of a statutory function – either immediately or in the longer term (for example, as part of ascertaining a pattern of behavior over time).

36. Information that is relevant to the performance of a function should be reassessed at regular intervals to determine whether it continues to be relevant. Relevant information might include information that is subsequently used in the compilation of a report, assessment, operational decision or other output of GCSB or NZSIS. Information that does not subsequently inform or become part of a report, assessment, operational decisions or other output is likely to be no longer relevant, and if so, should be disposed of in accordance with legal disposal authorities.

37. Assessments of necessity and relevance must also ensure that the information collected is lawful – ie in accordance with the scope of an authorisation or otherwise lawful collection method. Any material collected under a revoked urgent or very urgent authorisation, or information that is unauthorised or irrelevant (as defined in the Act), must be destroyed in accordance with the Act.

38. GCSB and NZSIS may retain incidentally obtained information that comes into the agency's possession and is not relevant to the performance of their statutory functions only for the purpose of disclosing it to another agency for the performance of that agency's statutory functions, in accordance with the requirements of section 104 of the Act. Information that is disclosed to the Police, New Zealand Defence Force or other public authority under section 104 should be disposed of as soon as possible after that disclosure, in accordance with legal disposal authorities and oversight requirements.

Shared responsibility

39. Information management is the shared responsibility of all employees, regardless of the role an employee plays in GCSB and NZSIS. Every employee must be aware of, and follow, information management policies and procedures in the course of their work. All employees have a general duty to create and capture full and accurate records, as well as to maintain and manage those records, in compliance with those policies and procedures.

Management of access

40. GCSB and NZSIS must ensure that access to all information is appropriately managed, with a strict regime of access controls applied. Access to information obtained by GCSB and NZSIS should be limited to the minimum number of people that are required to see it for the purposes of performing the statutory functions of the agencies. In other words, there must be a positive reason ("need-to-know") for access to information.

41. Access control systems and procedures must be in place to ensure that incorrect access permissions cannot be assigned, so as to avoid inadvertent access for those who are not required to view information. This includes having the ability to log who has accessed information and when, and being able to identify unauthorised access to information. Unauthorised access includes when an employee is authorised to access information but has done so for purposes other than to fulfill a statutory function which is within that employee's remit or has done so for the purposes of providing the information to an unauthorised party.

42. GCSB and NZSIS should also consider any access controls required once public records have been transferred to Archives New Zealand. Public service departments have an obligation to enable ongoing access to records under section 17(2) of the Public Records Act 2005. Under the Public Records Act, GCSB and NZSIS must set the access status of information and the period of any restrictions for records that are transferred to Archives New Zealand or that are 25 years old.

Security of information

43. All information obtained by GCSB and NZSIS must be stored in an appropriate repository/repositories, reflecting the sensitivity of the information and level of protections required. Electronic storage systems must be accredited in accordance with relevant standards outlined in the New Zealand Protective Security Requirements, and in the case of information gained from overseas public authorities, in accordance with the originators' requirements. The use of long-term digital storage systems should be subject to risk assessments that consider implications for future access to the information.
44. Differing levels of care and methods of storage will be required for differing types of information. GCSB and NZSIS will ensure that information is classified according to the New Zealand Government Security Classification System, and subsequent storage and handling requirements adhered to. GCSB and NZSIS will ensure the appropriate protections are place around information that is particularly sensitive, such as that relating to sensitive category individuals or security vetting records, or "need-to-know". This information may require a combination of limited access with additional password protections/encryptions (or similar protections).
45. In the case of information that has been retained for the purposes of disclosing to a third party under section 104 of the Act, GCSB and NZSIS must ensure the protection of that information up until the point it is disclosed to the third party (at which point the responsibility of protecting the information shifts to the third party), and if it is not disposed of immediately thereafter, until it is disposed of in accordance with legal disposal authorities.

Oversight

46. Effective information management practices are essential to facilitate effective oversight of GCSB and NZSIS by the Inspector-General of Intelligence and Security, as well as to support decisions to release/decline requests for access to information under the Privacy Act and Official Information Act. GCSB and NZSIS information management policies and procedures must be able to support effective responses to requests by the Inspector-General of Intelligence and Security, the Office of the Privacy Commissioner and the Office of the Ombudsman.

Additional matters to be reflected in internal policies and procedures

47. GCSB and NZSIS must have, and act in compliance with, internal policies and procedures that are consistent with the requirements and principles above, and must have systems in place to support and monitor compliance. Those policies and procedures must also address the following additional matters:

Recording and grading of information

Information retained by GCSB and NZSIS should be accurate, to the best knowledge of those recording it. To ensure this requirement is practicable, when information is subsequently proven to be false, steps should be taken to amend records still in the custody of the agencies to correct the inaccurate information.

GCSB and NZSIS must have procedures for recording information accurately and in a manner which will allow it to be used. This should include recording:

- the source of the information,
- the nature of the source,
- any assessment of the reliability of the source (where the reliability is not clear from the nature of the source), and
- any necessary restrictions on the use to be made of the information.

This information is required to support later review, reassessment and audit of the information and should be recorded in an agreed format which is used consistently across both agencies, where possible.

GCSB and NZSIS procedures for recording and grading information should also include lists of examples of information that is covered by various record classes (such as common corporate service public records as covered by General Disposal Authority 6 and facilitative, transitory and/or short-term value records as covered by General Disposal Authority 7), and guidance on determining authoritative versions of information (ie the authentic record) when information is stored in physical and digital form.

GCSB and NZSIS must specify default retention periods of different classes of information that is proportionate to the nature of the information and the purpose for which it was collected or created, and relevant legal obligations. Retention beyond default retention periods must be necessary for the performance of a statutory function.

Review, retention, destruction, and transfer schedules

GCSB and NZSIS must have schedules that provide for the following actions to occur at appropriate intervals:

- Review of retained information to ensure it continues to meet the necessity and relevance principle, ie is required to be retained for the purposes of fulfilling a statutory function, or is reasonably likely to be required for the purpose of fulfilling a statutory function in the future;
- Timely destruction of information as required by sections 76, 81, 102, 103, and 152 of the Act;
- Timely disposal of information that is covered by General Disposal Authorities 6 and 7 issued under the Public Records Act 2005 (it is important that records that no longer need to be kept are disposed of routinely in the normal course of business to minimise costs of maintaining and managing records);
- Identification and transfer of information of long-term value to Archives New Zealand, in accordance with statutory requirements under the Public Records Act 2005.

These schedules are to apply to all information collected by various means, not just information collected under a warrant. GCSB and NZSIS must develop with the Chief Archivist, approved retention and disposal schedules that allow for the disposal of information that is no longer relevant to the performance of the agencies' statutory functions. Statutory requirements to destroy certain information under the Intelligence and Security Act should be reflected in those disposal schedules. Those schedules may be agency-specific or sector-wide.

Privileged information

The law recognises certain types of privilege that attach to particular categories of information. Privileges recognise the public interest in protecting certain types of confidences. For example, legal advice privilege recognises the importance of the client being free of any disincentives to seeking legal advice and thereby being able to ensure his or her affairs are compliant with the law. The Evidence Act 2006 privileges that are protected under the Intelligence and Security Act comprise legal advice privilege, litigation privilege, religious privilege and medical privilege and the privilege for settlement negotiations and mediation. GCSB and NZSIS employees should also be aware of when Parliamentary privilege and the protection for journalists' sources may apply.

GCSB and NZSIS are prohibited from obtaining some types of privileged communications or privileged information of New Zealanders and permanent residents of New Zealand under intelligence warrants, however there may be times when such information is inadvertently collected. GCSB and NZSIS must have policies in place which address the need to protect statutorily prescribed classes of privileged information to ensure the protections that apply in relation to that information are complied with. These protections include the obligation to destroy (without reporting) any privileged material relating to New Zealanders that is inadvertently intercepted. The Directors-General must ensure that all employees receive training on the nature of relevant privileges and the applicable policies.

Audit procedures

GCSB and NZSIS must conduct periodic internal audits to ensure relevant policies and procedures associated with assessments of relevance, access to, retention, disposal, destruction and transfer of information held by GCSB and NZSIS are being adhered to. GCSB and NZSIS should consult with the Department of Internal Affairs (Archives New Zealand) in developing audit procedures. GCSB and NZSIS will also be subject to the audit review cycle conducted by the Chief Archivist.

Compliance with the information privacy principles

GCSB and NZSIS are subject to information privacy principles 1, 4(a), and 5 to 12 of the information privacy principles in the Privacy Act 1993. All policies relating to the management of personal information obtained by GCSB and NZSIS must incorporate guidance about compliance with the information privacy principles. The information privacy principles are relevant to policies relating to access, accuracy, security, use and disclosure, and retention of personal information by GCSB and NZSIS.

Information sharing

GCSB and NZSIS must have in place protocols for sharing information within and between agencies that are consistent with the principles of necessity and accessibility.

Procedures must also be in place for the disclosure of information to other government departments, as provided for under section 104 of the Act. These procedures should help

guide decision-making on what is relevant to disclose, the extent of information to be disclosed, and methods of disclosure.

Information sharing arrangements that involve the sharing of personal information must also comply with the Privacy Act 1993, either in accordance with the information privacy principles or under an approved information sharing agreement, except where there is another statutory authorisation provision or process.

GCSB and NZSIS must specify the protection, storage and use requirements that overseas public authorities are expected to adhere to in relation to information provided to them by GCSB and NZSIS. This should include any requirements or restrictions related to those authorities passing on that information to any third parties. Those requirements will be consistent with the principles in this MPS and the MPS on *Cooperation with overseas public authorities*.

It is recognised that the overseas public authority may be subject to its own national requirements for managing received information, which may conflict with conditions imposed by GCSB or NZSIS. GCSB and NZSIS should seek to be consulted by the overseas public authority regarding any requirements that may lead to shared information being used in a manner that conflicts with restrictions that would apply in New Zealand.

Training

All employees of GCSB and NZSIS must be provided compulsory training on all relevant law, policies and procedures in relation to information management, including privilege (as discussed above). This training should be provided to all existing employees and to new employees at induction, and whenever there are changes or updates to the policies and procedures, to ensure that at all times employees are aware of current practices.

Compliance with State Services Code of Conduct

The Directors-General of GCSB and NZSIS must issue policies and procedures that reflect their agencies' obligations under the State Sector Act 1988.

Authorisation procedures

48. The Directors-General of GCSB and NZSIS are to issue the policies and procedures to guide information management by the agencies. Disposal actions must only be taken in accordance with approved Disposal Authorities (general or agency-specific) issued by the Chief Archivist, or as otherwise required by law.

Duration of ministerial policy statement

49. This MPS will take effect from 28 September 2017 for a period of three years. The Minister who issued an MPS may, at any time, amend, revoke or replace the MPS.

Ministerial Policy Statement issued by:

Hon Christopher Finlayson
Minister responsible for the Government Communications Security Service
Minister in charge of the New Zealand Security Intelligence Service

September 2017