STATE SERVICES COMMISSION
Te Komihana O Ngā Tari Kāwanatanga

1 August 2018

[redacted]

Dear [redacted]

Official Information Request

Our Ref: SSC2018/0115

I refer to your official information request to the Department of Prime Minister and Cabinet, which was transferred to the State Services Commission (SSC) for response on 10 July 2018 and asks for copies of:

- *Cabinet Committee Minute EXG (00) M 20/7 and*
- *CAB (00) M42/4G(4)*
- *Cabinet Directive CAB MIN (14) 39/38.*

You also have requested:

- *Confirmation of whether the New Zealand Information Security Manual (NZISM) is binding on the New Zealand Defence Force, and if so the legislative or other basis for that status and a copy of the relevant authority (Cabinet Minute, for example) if it is not otherwise publicly available.*

Information being released

Please find enclosed the following documents you have requested which contain the information you have requested.

Item	Document Description	Decision
1	EXG (00) M 20/7 – Protection of Official Information	Released in full
2	CAB (00) M 42/4G(4) – Protection of Official Information	Released in full
3	CAB MIN (14) 39/38 – Protective Security Requirements	Released in full

In response to the second part of your request, Section 1.2.3 of the NZISM outlines that the manual applies to New Zealand Government departments, agencies and organisations as listed in:

- Parts 1 and 2 of Schedule 1 to the Ombudsmen Act 1975 (as amended)
- Schedule 1 to the Official Information Act 1982
- any other organisations that have entered into a formal Agreement with the New Zealand Government to have access to classified information.

The NZISM applies to the New Zealand Defence Force (NZDF) as they are one of the above organisations.

2 The Terrace
PO Box 329 Wellington 6140
New Zealand
Phone +64-4-495 6600
Fax +64-4-495 6686
www.ssc.govt.nz

Section 1.2.6 of the NZISM states: *The NZISM is intended to structure and assist the implementation of government policy that requires departments and agencies to protect the privacy, integrity and confidentiality of the information they collect, process, store and archive. While these overarching requirements are mandatory for departments and agencies, compliance with the NZISM is not required as a matter of law. The controls in the NZISM could be made binding on departments and agencies, either by legislation, or Cabinet direction.*

The Protective Security Requirements Framework provides a specific authority and mandate through a Cabinet Directive CAB MIN (14) 39/38.

If you wish to discuss this decision with us, please feel free to contact Ministerial.Services@ssc.govt.nz.

Please note that we intend to publish this letter (with your personal details removed) and enclosed documents on the State Services Commission's website.

Yours sincerely

Stephen Moore
Managing Principal
State Services Commission

CABINET COMMITTEE ON GOVERNMENT EXPENDITURE AND ADMINISTRATION

EXG (00) M 20/7

Copy No: 38

MINUTES of a meeting of the Committee held on **Wednesday, 113 December 2000 at 11.45am.**

PRESENT:	Hon Jim Anderton	CABINET MINUTE NOTED
	Hon Dr Michael Cullen	Commissioner:
	Hon Trevor Mallard (Chair)	Deputy Commissioner SSC:
	Hon Pete Hodgson	Deputy Commissioner:
	Hon George Hawkins	Legal Branch:
	Hon Mark Burton	
	Hon Paul Swain	
ALSO PRESENT:	Hon Marian Hobbs	
IN ATTENDANCE:	Officials from	Department of the Prime Minister and Cabinet Treasury

Protection of Official Information

Reference: EXG (00) 124

The Committee **agreed** to recommend that Cabinet:

a note that the system for protecting official information was last reviewed by Cabinet in 1982;

b note that the present system has a number of deficiencies:

i it provides rules that are mainly applicable to official information that requires protection for national security reasons, but does not adequately cover information that needs protection for other reasons, such as preserving personal privacy or avoiding the premature disclosure of government decision-making;

ii it operates effectively in a paper environment, but less so in a world where information is increasingly being held and transferred electronically;

iii it leads to over-classification of official information and expenditure on protective measures greater than warranted;

All Branch Managers

c agree that these deficiencies can be overcome by a revised system that:

i introduces a new framework for official information requiring protection for public interest and personal privacy reasons with security classifications of SENSITIVE and IN CONFIDENCE:

ii preserves the existing security classifications of TOP SECRET, SECRET and CONFIDENTIAL for information associated with national security, and adds a further classification of RESTRICTED;

d note that the revised system for protecting official information will be consistent with, and not replace, the obligations contained in the Official Information Act 1982;

e agree that the revised system be introduced within government departments, ministerial offices, the NZ Police, the NZ Defence Force, the NZ Security Intelligence Service and the Government Communications Security Bureau, and also be made available to state owned enterprises and crown entities;

f agree that the guidelines for grading information as SENSITIVE, IN CONFIDENCE, TOP SECRET, SECRET, CONFIDENTIAL and RESTRICTED be as shown in Appendix 1 to this minute;

g agree that chief executives will be responsible for setting the levels of protection for RESTRICTED, SENSITIVE and IN CONFIDENCE information using a risk management approach and taking into account a minimum level to be applied across all departments, as shown in the guidelines attached as Appendix 2 to this minute;

h direct the State Services Commission and the Department of Prime Minister and Cabinet to coordinate the implementation of the revised system, including the reissue of the manual *Security in Government Departments,* to reflect the above policy;

i agree that a Cabinet Office circular be issued to advise ministerial offices and departments of the implementation of the new requirements in relation to the submission of papers for Cabinet;

j note that implementation of the revised system will occur over a two year period commencing in February 2001;

k note that the costs incurred in implementing the revised system will be accommodated within existing baselines.

Brian Hallinan
Secretary

COPIES TO: (See Over)

COPIES TO:

Cabinet Committee on Government Expenditure and Administration
Chief Executive, DPMC
B Wilson, DPMC
Director, Domestic and External Security Secretariat
Director, New Zealand Security Intelligence Service
Director, Government Communications Security Bureau
Chief Executive, Ministry of Economic Development
Secretary to the Treasury
A Kibblewhite, Treasury
Commissioner of Inland Revenue
Minister of Social Services and Employment
Chief Executive, Department of Work and Income
Minister of Foreign Affairs and Trade
Secretary of Foreign Affairs and Trade
Secretary for Justice
Minister of Justice (Privacy Commissioner)
State Services Commissioner
Commissioner of Police
Secretary of Defence
Chief of Defence Force

PROTECTION OF OFFICIAL INFORMATION

SECURITY CLASSIFICATIONS

INTRODUCTION

This Appendix provides guidelines for selecting an appropriate security classification where it has been determined that official information requires protection using specific handling rules. It is emphasised that the guidelines are not prescriptive; rather they are provided to assist in the classification process. **The classification will be chosen by the responsible departmental staff member through reference to content and the degree of damage or prejudice that would arise from disclosure of the information.**

The two new classifications, **SENSITIVE** and **IN CONFIDENCE**, cover information requiring protection for public interest and personal privacy reasons. Guidelines for grading information as **SENSITIVE** or **IN CONFIDENCE** draw on the reasons in the Official Information Act 1982 for withholding official information.

The three existing classifications **TOP SECRET, SECRET, CONFIDENTIAL,** and a new classification **RESTRICTED** cover information requiring protection for national security reasons; that is situations where making information available would be likely to:

- prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand
- prejudice the entrusting of information to the Government of New Zealand on a basis of confidence by the government of any other country, or any agency of a such a government, or any international organisation

Guidelines for grading information as **TOP SECRET, SECRET** or **CONFIDENTIAL** are in essence unchanged, although they have been made more explicit to assist in their application. The guidelines covering **RESTRICTED** are new. All of these guidelines are similar to those in use by Australia.

IMPORTANT NOTE

The Official Information Act allows information to be protected to the extent consistent with the public interest and the preservation of personal privacy.

Classifications are used to grade information on the basis of the damage that would result from unauthorised disclosure and to specify the protective measures to be applied.

In themselves, classifications do not allow official information to be withheld; rather, the information must be considered on its merits using the criteria in the Act.

GUIDELINES FOR SENSITIVE AND IN CONFIDENCE

The following guidelines are for grading information as SENSITIVE or IN CONFIDENCE.

Most information will be adequately protected by the classification IN CONFIDENCE.

Some information will warrant the higher classification SENSITIVE through reference to content and the degree of damage or prejudice that would arise from its disclosure.

SENSITIVE	Compromise of information would be likely to damage the interests of the New Zealand government or endanger the safety of its citizens

Any information that meets the following guidelines will usually be classified as SENSITIVE. In addition, any information covered by the guidelines for IN CONFIDENCE (see next page) should be classified as SENSITIVE, where a determination by subject matter and degree of damage or prejudice that would arise from its disclosure indicates that a greater level of protection is warranted.

- endanger the safety of any person
- damage seriously the economy of New Zealand by disclosing prematurely decisions to change or continue Government economic or financial policies relating to:
  - exchange rates or the control of overseas exchange transactions
  - the regulation of banking or credit
  - taxation
  - the stability, control, and adjustment of prices of goods and services, rents, and other costs, and rates of wages, salaries, and other incomes
  - the borrowing of money by the Government of New Zealand
  - the entering into of overseas trade agreements
- impede a Minister of the Crown or an Department or organisation holding the information to carry on without prejudice or disadvantage, negotiations (including commercial and industrial negotiations)

IN CONFIDENCE	Compromise of information would be likely to prejudice the maintenance of law and order, impede the effective conduct of government in New Zealand or affect adversely the privacy of its citizens

Any information that meets the following guidelines will usually be classified IN CONFIDENCE unless a determination by subject matter and degree of damage or prejudice that would arise from its disclosure indicates that a greater level of protection is warranted. If so, the higher classification SENSITIVE should be used.

- prejudice the maintenance of the law, including the prevention, investigation, and detection of offences, and the right to a fair trial
- affect adversely the privacy of natural persons, including that of deceased natural persons
- disclose a trade secret or unreasonably to prejudice the commercial position of the person who supplied or is the subject of the information
- disclose information which is subject to an obligation of confidence or which any person has been or could be compelled to provide under the authority of any enactment, where the making available of the information would:
  - be likely to prejudice the supply of similar information, or information from the same source, and it is in the public interest that such information should continue to be supplied
  - be likely otherwise to damage the public interest
- prejudice measures protecting the health or safety of members of the public
- prejudice the substantial economic interests of New Zealand
- prejudice measures that prevent or mitigate material loss to members of the public
- breach the constitutional conventions for the time being which protect:
  - the confidentiality of communications by or with the Sovereign or her representative
  - collective and individual ministerial responsibility
  - the political neutrality of officials
  - the confidentiality of advice tendered by Ministers of the Crown and officials
- impede the effective conduct of public affairs through:
  - the free and frank expression of opinions by or between or to Ministers of the Crown or officers and employees of any department or organisation in the course of their duty
  - the protection of such Ministers, officers and employees from improper pressure or harassment
- breach legal professional privilege
- impede a Minister of the Crown or any Department or organisation holding the information to carry out, without prejudice or disadvantage, commercial activities
- lead to the disclosure or use of official information for improper gain or advantage

- *NB: Information held internally by a department that is classified as IN CONFIDENCE may not always be labelled as such. It should be so marked, however, whenever it is passed outside the department to ensure that it is afforded appropriate protection.*

GUIDELINES FOR TOP SECRET, SECRET,CONFIDENTIAL AND RESTRICTED

These four classifications cover information that requires protection for national security reasons. Most national security information would be adequately protected by the classifications CONFIDENTIAL or RESTRICTED. The classification SECRET should be used sparingly. Very little national security information warrants the classification TOP SECRET, which should be used with the utmost restraint.

TOP SECRET	Compromise of information would damage national interests in an exceptionally grave manner

- threaten directly the internal stability of New Zealand or friendly countries
- lead directly to widespread loss of life
- cause exceptionally grave damage to the operational effectiveness or security of New Zealand or friendly forces or to the continuing effectiveness of extremely valuable security or intelligence operations
- cause exceptionally grave damage to relations with other governments
- cause severe long term damage to significant national infrastructure

SECRET	Compromise of information would damage national interests in a serious manner

- raise international tension
- damage seriously relations with friendly governments
- cause serious damage to the operational effectiveness or security of New Zealand or friendly forces or the effectiveness of valuable security or intelligence operations
- seriously damage the internal stability of New Zealand or friendly countries
- shut down or substantially disrupt significant national infrastructure

CONFIDENTIAL	Compromise of information would damage national interests in a significant manner

- materially damage diplomatic relations (i.e. cause formal protest or other sanction)
- cause damage to the operational effectiveness or security of New Zealand or friendly forces or to the continuing effectiveness of valuable security or intelligence operations
- damage the internal stability of New Zealand or friendly countries
- disrupt significant national infrastructure

RESTRICTED	Compromise of information would be likely to affect the national interest in an adverse manner

- affect diplomatic relations adversely
- hinder the operational effectiveness or security of New Zealand or friendly forces
- affect the internal stability or economic well-being of New Zealand or friendly countries adversely

GUIDELINES for HANDLING RESTRICTED, SENSITIVE or IN CONFIDENCE INFORMATION

INTRODUCTION

Chief Executives are responsible for determining the levels of protection for RESTRICTED, SENSITIVE or IN CONFIDENCE[1] information to be applied within their departments. A Risk Management[2] approach is to be taken to achieve the protection as cost effectively as possible. The following publications are to be used as guidelines:

- The New Zealand Security of Information Technology (SIT) series of Publications issued by the Government Communications Security Bureau (GCSB).
- AS/NZ Standard 4444: *Information Security Management* and AS/NZ Standard: *Information Security Risk Management* (yet to be issued).

The levels of protection are to ensure that:

- Information should be held, processed, transmitted and destroyed with discretion to avoid opportunistic access by unauthorised people and make accidental compromise highly unlikely.
- All obligations to protect information provided by third parties are met.
- The release of RESTRICTED, SENSITIVE or IN CONFIDENCE information outside Government places it at no greater risk than if the Department concerned continued to hold it.
- Departmental staff are told about the level of protection required. Those outside Government should also be given similar guidance.

[1] This Appendix provides guidelines for protecting RESTRICTED, SENSITIVE and IN CONFIDENCE information. The rules for protecting TOP SECRET, SECRET and CONFIDENTIAL information are unchanged and contained in the manual *Security in Government Departments*.

[2] Risk management as defined in the Australia/New Zealand Standard 4360 – Risk Management

HANDLING AND/OR TRANSMISSION OF 'RESTRICTED' OR 'SENSITIVE' INFORMATION

Principles and clearance level	▪ Information classified as RESTRICTED or SENSITIVE should be held, processed, transmitted and destroyed with discretion to make compromise highly unlikely. ▪ Only staff cleared by the department to access RESTRICTED or SENSITIVE level or above are authorised to handle the information. This includes all staff involved with transmission, storage, and disposal.

ELECTRONIC TRANSMISSION	▪ All RESTRICTED or SENSITIVE information transmitted across public networks within New Zealand or across any networks overseas must be encrypted using a system approved by the GCSB.
ELECTRONIC STORAGE	▪ Electronic files (including databases) must be protected against illicit internal use or intrusion by external parties through a judicious selection of two or more of the following mechanisms: - User challenge and authentication (username/password or digital ID/certificate) - Logging use at level of individual - Firewalls and intrusion detection systems and procedures - Server authentication - OS-specific /application-specific security measures - Encryption
ELECTRONIC DISPOSAL	▪ Electronic files should be disposed of in a way that makes reconstruction highly unlikely.
PAPER TRANSMISSION	▪ May be carried by ordinary postal services including commercial courier firms, provided the envelope/package is sealed and the word RESTRICTED or SENSITIVE is not visible. ▪ The outer envelope should be addressed to an individual by name and title. RESTRICTED or SENSITIVE mail for/from overseas should be carried by diplomatic airfreight. ▪ The outer envelope must clearly show a return address in case delivery is unsuccessful. In some cases due to the nature of the contents, identifying the originating department may be inappropriate and a return PO Box alone should be used.
PAPER STORAGE	▪ Follow storage guidelines in *Data Management Standard for NZ Government* or Archives NZ Storage Standard NAS 9901 *Storage of Public Records or Archives* or in-house Records Management policy.
PAPER DISPOSAL	▪ Disposed of or destroyed in a way that makes reconstruction highly unlikely.

HANDLING AND/OR TRANSMISSION OF 'IN CONFIDENCE' INFORMATION

Principles and clearance level	▪ Information for official use, with consideration of 'need to know' principle

ELECTRONIC TRANSMISSION	▪ An appropriate statement should accompany all IN CONFIDENCE information transmitted via e-mail or Fax. ▪ It should outline legal responsibilities and notification/destruction instructions if the incorrect party receives it. ▪ IN CONFIDENCE data can be transmitted across external or public networks but the level of information contained should be assessed before using clear text. ▪ Username/Password access control and/or encryption may be advisable (with the aim of maintaining public confidence in government agencies). ▪ All IN CONFIDENCE information (including data) should clearly identify the originating government agency and date.
ELECTRONIC STORAGE	▪ Electronic files (including databases) should be protected against illicit internal use or intrusion by external parties through two or more of the following mechanisms: - User challenge and authentication (username/password or digital ID/certificate) - Logging use at level of individual - Firewalls and intrusion detection systems and procedures - Server authentication - OS-specific /application-specific security measures.
ELECTRONIC DISPOSAL	▪ Electronic files should be disposed of in a way that makes reconstruction highly unlikely.
PAPER TRANSMISSION	▪ May be carried by ordinary postal services or commercial courier firms as well as mail delivery staff in a single sealed envelope. ▪ The envelope must clearly show a return address in case delivery is unsuccessful. In some cases involving privacy concerns, identifying the originating department may be inappropriate and a return PO Box alone should be used.
PAPER STORAGE	▪ IN CONFIDENCE information can be secured using the normal building security and door-swipe card systems that aim simply to keep the public out of administrative areas of government departments. ▪ It should be noted that IN CONFIDENCE material may not always be labelled as such, particularly where it is never passed outside the responsible department.
PAPER DISPOSAL	▪ Disposed of by departmental arrangement that make compromise highly unlikely.

CABINET

CAB (00) M 42/4G(4)

This paper is the property of the New Zealand Government. As it includes material for Cabinet or Cabinet Committee purposes it must be handled with particular care, and in accordance with any security classification or other endorsement assigned to it. The information in it may be released only by persons having proper authority to do so, and strictly in terms of that authority.

Minister of State Services

CABINET MINUTE NOTED
Commissioner: _____
Deputy Commissioner SSC: _____
Deputy Commissioner: _____
Legal Branch: _____

COPIES TO:

Prime Minister
Deputy Prime Minister
All Ministers
All Chief Executives
Speaker of the House
Chair Parliamentary Service Commission
Controller and Auditor-General
Chief Parliamentary Counsel
Secretary of the Cabinet
Secretary, EXG

Protection of Official Information

All Branch Managers

Reference: CAB (00) 843; EXG (00) M 20/7

At the meeting on 18 December 2000, following reference from the Cabinet Committee on Government Expenditure and Administration, Cabinet:

a **noted** that the system for protecting official information was last reviewed by Cabinet in 1982;

b **noted** that the present system has a number of deficiencies:

i it provides rules that are mainly applicable to official information that requires protection for national security reasons, but does not adequately cover information that needs protection for other reasons, such as preserving personal privacy or avoiding the premature disclosure of government decision-making;

ii it operates effectively in a paper environment, but less so in a world where information is increasingly being held and transferred electronically;

iii it leads to over-classification of official information and expenditure on protective measures greater than warranted;

c **agreed** that these deficiencies can be overcome by a revised system that:

i introduces a new framework for official information requiring protection for public interest and personal privacy reasons with security classifications of SENSITIVE and IN CONFIDENCE:

ii preserves the existing security classifications of TOP SECRET, SECRET and CONFIDENTIAL for information associated with national security, and adds a further classification of RESTRICTED;

d **noted** that the revised system for protecting official information will be consistent with, and not replace, the obligations contained in the Official Information Act 1982;

e **agreed** that the revised system be introduced within government departments, ministerial offices, the NZ Police, the NZ Defence Force, the NZ Security Intelligence Service and the Government Communications Security Bureau, and also be made available to state owned enterprises and crown entities;

f **agreed** that the guidelines for grading information as SENSITIVE, IN CONFIDENCE, TOP SECRET, SECRET, CONFIDENTIAL and RESTRICTED be as shown in Annex 1 to this minute;

g **agreed** that chief executives will be responsible for setting the levels of protection for RESTRICTED, SENSITIVE and IN CONFIDENCE information using a risk management approach and taking into account a minimum level to be applied across all departments, as shown in the guidelines attached as Annex 2 to this minute;

h **directed** the State Services Commission and the Department of Prime Minister and Cabinet to coordinate the implementation of the revised system, including the reissue of the manual *Security in Government Departments,* to reflect the above policy;

i **agreed** that a Cabinet Office circular be issued to advise ministerial offices and departments of the implementation of the new requirements in relation to the submission of papers for Cabinet;

j **noted** that implementation of the revised system will occur over a two year period commencing in February 2001;

k **noted** that the costs incurred in implementing the revised system will be accommodated within existing baselines.

Secretary of the Cabinet

PROTECTION OF OFFICIAL INFORMATION

SECURITY CLASSIFICATIONS

INTRODUCTION

This Appendix provides guidelines for selecting an appropriate security classification where it has been determined that official information requires protection using specific handling rules. It is emphasised that the guidelines are not prescriptive; rather they are provided to assist in the classification process. **The classification will be chosen by the responsible departmental staff member through reference to content and the degree of damage or prejudice that would arise from disclosure of the information.**

The two new classifications, **SENSITIVE** and **IN CONFIDENCE**, cover information requiring protection for public interest and personal privacy reasons. Guidelines for grading information as **SENSITIVE** or **IN CONFIDENCE** draw on the reasons in the Official Information Act 1982 for withholding official information.

The three existing classifications **TOP SECRET, SECRET, CONFIDENTIAL,** and a new classification **RESTRICTED** cover information requiring protection for national security reasons; that is situations where making information available would be likely to:

- prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand
- prejudice the entrusting of information to the Government of New Zealand on a basis of confidence by the government of any other country, or any agency of a such a government, or any international organisation

Guidelines for grading information as **TOP SECRET, SECRET** or **CONFIDENTIAL** are in essence unchanged, although they have been made more explicit to assist in their application. The guidelines covering **RESTRICTED** are new. All of these guidelines are similar to those in use by Australia.

IMPORTANT NOTE

The Official Information Act allows information to be protected to the extent consistent with the public interest and the preservation of personal privacy.

Classifications are used to grade information on the basis of the damage that would result from unauthorised disclosure and to specify the protective measures to be applied.

In themselves, classifications do not allow official information to be withheld; rather, the information must be considered on its merits using the criteria in the Act.

GUIDELINES FOR SENSITIVE AND IN CONFIDENCE

The following guidelines are for grading information as SENSITIVE or IN CONFIDENCE.

Most information will be adequately protected by the classification IN CONFIDENCE.

Some information will warrant the higher classification SENSITIVE through reference to content and the degree of damage or prejudice that would arise from its disclosure.

SENSITIVE	Compromise of information would be likely to damage the interests of the New Zealand government or endanger the safety of its citizens

Any information that meets the following guidelines will usually be classified as SENSITIVE. In addition, any information covered by the guidelines for IN CONFIDENCE (see next page) should be classified as SENSITIVE, where a determination by subject matter and degree of damage or prejudice that would arise from its disclosure indicates that a greater level of protection is warranted.

- endanger the safety of any person
- damage seriously the economy of New Zealand by disclosing prematurely decisions to change or continue Government economic or financial policies relating to:
  - exchange rates or the control of overseas exchange transactions
  - the regulation of banking or credit
  - taxation
  - the stability, control, and adjustment of prices of goods and services, rents, and other costs, and rates of wages, salaries, and other incomes
  - the borrowing of money by the Government of New Zealand
  - the entering into of overseas trade agreements
- impede a Minister of the Crown or an Department or organisation holding the information to carry on without prejudice or disadvantage, negotiations (including commercial and industrial negotiations)

IN CONFIDENCE	Compromise of information would be likely to prejudice the maintenance of law and order, impede the effective conduct of government in New Zealand or affect adversely the privacy of its citizens

Any information that meets the following guidelines will usually be classified IN CONFIDENCE unless a determination by subject matter and degree of damage or prejudice that would arise from its disclosure indicates that a greater level of protection is warranted. If so, the higher classification SENSITIVE should be used.

- prejudice the maintenance of the law, including the prevention, investigation, and detection of offences, and the right to a fair trial
- affect adversely the privacy of natural persons, including that of deceased natural persons
- disclose a trade secret or unreasonably to prejudice the commercial position of the person who supplied or is the subject of the information
- disclose information which is subject to an obligation of confidence or which any person has been or could be compelled to provide under the authority of any enactment, where the making available of the information would:
  - be likely to prejudice the supply of similar information, or information from the same source, and it is in the public interest that such information should continue to be supplied
  - be likely otherwise to damage the public interest
- prejudice measures protecting the health or safety of members of the public
- prejudice the substantial economic interests of New Zealand
- prejudice measures that prevent or mitigate material loss to members of the public
- breach the constitutional conventions for the time being which protect:
  - the confidentiality of communications by or with the Sovereign or her representative
  - collective and individual ministerial responsibility
  - the political neutrality of officials
  - the confidentiality of advice tendered by Ministers of the Crown and officials
- impede the effective conduct of public affairs through:
  - the free and frank expression of opinions by or between or to Ministers of the Crown or officers and employees of any department or organisation in the course of their duty
  - the protection of such Ministers, officers and employees from improper pressure or harassment
- breach legal professional privilege
- impede a Minister of the Crown or any Department or organisation holding the information to carry out, without prejudice or disadvantage, commercial activities
- lead to the disclosure or use of official information for improper gain or advantage

- *NB: Information held internally by a department that is classified as IN CONFIDENCE may not always be labelled as such. It should be so marked, however, whenever it is passed outside the department to ensure that it is afforded appropriate protection.*

GUIDELINES FOR TOP SECRET, SECRET,CONFIDENTIAL AND RESTRICTED

These four classifications cover information that requires protection for national security reasons. Most national security information would be adequately protected by the classifications CONFIDENTIAL or RESTRICTED. The classification SECRET should be used sparingly. Very little national security information warrants the classification TOP SECRET, which should be used with the utmost restraint.

TOP SECRET	Compromise of information would damage national interests in an exceptionally grave manner

- threaten directly the internal stability of New Zealand or friendly countries
- lead directly to widespread loss of life
- cause exceptionally grave damage to the operational effectiveness or security of New Zealand or friendly forces or to the continuing effectiveness of extremely valuable security or intelligence operations
- cause exceptionally grave damage to relations with other governments
- cause severe long term damage to significant national infrastructure

SECRET	Compromise of information would damage national interests in a serious manner

- raise international tension
- damage seriously relations with friendly governments
- cause serious damage to the operational effectiveness or security of New Zealand or friendly forces or the effectiveness of valuable security or intelligence operations
- seriously damage the internal stability of New Zealand or friendly countries
- shut down or substantially disrupt significant national infrastructure

CONFIDENTIAL	Compromise of information would damage national interests in a significant manner

- materially damage diplomatic relations (i.e. cause formal protest or other sanction)
- cause damage to the operational effectiveness or security of New Zealand or friendly forces or to the continuing effectiveness of valuable security or intelligence operations
- damage the internal stability of New Zealand or friendly countries
- disrupt significant national infrastructure

RESTRICTED	Compromise of information would be likely to affect the national interest in an adverse manner

- affect diplomatic relations adversely
- hinder the operational effectiveness or security of New Zealand or friendly forces
- affect the internal stability or economic well-being of New Zealand or friendly countries adversely

GUIDELINES for HANDLING RESTRICTED, SENSITIVE or IN CONFIDENCE INFORMATION

INTRODUCTION

Chief Executives are responsible for determining the levels of protection for RESTRICTED, SENSITIVE or IN CONFIDENCE[1] information to be applied within their departments. A Risk Management[2] approach is to be taken to achieve the protection as cost effectively as possible. The following publications are to be used as guidelines:

- The New Zealand Security of Information Technology (SIT) series of Publications issued by the Government Communications Security Bureau (GCSB).
- AS/NZ Standard 4444: *Information Security Management* and AS/NZ Standard: *Information Security Risk Management* (yet to be issued).

The levels of protection are to ensure that:

- Information should be held, processed, transmitted and destroyed with discretion to avoid opportunistic access by unauthorised people and make accidental compromise highly unlikely.
- All obligations to protect information provided by third parties are met.
- The release of RESTRICTED, SENSITIVE or IN CONFIDENCE information outside Government places it at no greater risk than if the Department concerned continued to hold it.
- Departmental staff are told about the level of protection required. Those outside Government should also be given similar guidance.

[1] This Appendix provides guidelines for protecting RESTRICTED, SENSITIVE and IN CONFIDENCE information. The rules for protecting TOP SECRET, SECRET and CONFIDENTIAL information are unchanged and contained in the manual *Security in Government Departments*.

[2] Risk management as defined in the Australia/New Zealand Standard 4360 – Risk Management

HANDLING AND/OR TRANSMISSION OF 'RESTRICTED' OR 'SENSITIVE' INFORMATION

Principles and clearance level	▪ Information classified as RESTRICTED or SENSITIVE should be held, processed, transmitted and destroyed with discretion to make compromise highly unlikely. ▪ Only staff cleared by the department to access RESTRICTED or SENSITIVE level or above are authorised to handle the information. This includes all staff involved with transmission, storage, and disposal.

ELECTRONIC TRANSMISSION	▪ All RESTRICTED or SENSITIVE information transmitted across public networks within New Zealand or across any networks overseas must be encrypted using a system approved by the GCSB.
ELECTRONIC STORAGE	▪ Electronic files (including databases) must be protected against illicit internal use or intrusion by external parties through a judicious selection of two or more of the following mechanisms: - User challenge and authentication (username/password or digital ID/certificate) - Logging use at level of individual - Firewalls and intrusion detection systems and procedures - Server authentication - OS-specific/application-specific security measures - Encryption
ELECTRONIC DISPOSAL	▪ Electronic files should be disposed of in a way that makes reconstruction highly unlikely.
PAPER TRANSMISSION	▪ May be carried by ordinary postal services including commercial courier firms, provided the envelope/package is sealed and the word RESTRICTED or SENSITIVE is not visible. ▪ The outer envelope should be addressed to an individual by name and title. RESTRICTED or SENSITIVE mail for/from overseas should be carried by diplomatic airfreight. ▪ The outer envelope must clearly show a return address in case delivery is unsuccessful. In some cases due to the nature of the contents, identifying the originating department may be inappropriate and a return PO Box alone should be used.
PAPER STORAGE	▪ Follow storage guidelines in *Data Management Standard for NZ Government* or Archives NZ Storage Standard NAS 9901 *Storage of Public Records or Archives* or in-house Records Management policy.
PAPER DISPOSAL	▪ Disposed of or destroyed in a way that makes reconstruction highly unlikely.

HANDLING AND/OR TRANSMISSION OF 'IN CONFIDENCE' INFORMATION

Principles and clearance level	▪ Information for official use, with consideration of 'need to know' principle

ELECTRONIC TRANSMISSION	▪ An appropriate statement should accompany all IN CONFIDENCE information transmitted via e-mail or Fax. ▪ It should outline legal responsibilities and notification/destruction instructions if the incorrect party receives it. ▪ IN CONFIDENCE data can be transmitted across external or public networks but the level of information contained should be assessed before using clear text. ▪ Username/Password access control and/or encryption may be advisable (with the aim of maintaining public confidence in government agencies). ▪ All IN CONFIDENCE information (including data) should clearly identify the originating government agency and date.
ELECTRONIC STORAGE	▪ Electronic files (including databases) should be protected against illicit internal use or intrusion by external parties through two or more of the following mechanisms: - User challenge and authentication (username/password or digital ID/certificate) - Logging use at level of individual - Firewalls and intrusion detection systems and procedures - Server authentication - OS-specific /application-specific security measures.
ELECTRONIC DISPOSAL	▪ Electronic files should be disposed of in a way that makes reconstruction highly unlikely.
PAPER TRANSMISSION	▪ May be carried by ordinary postal services or commercial courier firms as well as mail delivery staff in a single sealed envelope. ▪ The envelope must clearly show a return address in case delivery is unsuccessful. In some cases involving privacy concerns, identifying the originating department may be inappropriate and a return PO Box alone should be used.
PAPER STORAGE	▪ IN CONFIDENCE information can be secured using the normal building security and door-swipe card systems that aim simply to keep the public out of administrative areas of government departments. ▪ It should be noted that IN CONFIDENCE material may not always be labelled as such, particularly where it is never passed outside the responsible department.
PAPER DISPOSAL	▪ Disposed of by departmental arrangement that make compromise highly unlikely.

Cabinet

CAB Min (14) 39/38

Copy No: 30

Minute of Decision

Protective Security Requirements

Portfolios: Prime Minister/ State Services/ NZSIS/ GCSB

On 8 December 2014, following reference from the Cabinet Committee on State Sector Reform and Expenditure Control, Cabinet:

1 **noted** that government departments face diverse and complex threats to the security of their people, information and assets;

2 **noted** that existing security advice for government departments is fragmented and not implemented effectively;

3 **noted** that it is proposed that a new Protective Security Requirements (PSR) framework replace the current multiple manuals so as to provide a single source of better tools and guidance for departments as they implement the requirements;

4 **noted** that the Protective Security Requirements (PSR) will contain 29 mandatory security requirements for government departments relating to governance, personnel, information and physical assets;

5 **noted** that the PSR have been developed in consultation with a broad range of departments, including road-testing the requirements with six departments;

6 **noted** that the PSR have been developed in close coordination with the Government Chief Information Officer and the Government Chief Privacy Officer and that the guidance and requirements for privacy and security are aligned and not duplicative;

7 **noted** that the PSR team, working closely with the Government Communications Security Bureau, the New Zealand Security and Intelligence Service, and the Department of the Prime Minister and Cabinet (lead security agencies), will provide guidance and support to departments on the implementation of the PSR;

8 **agreed** to adopt the PSR, incorporating the updated *New Zealand Information Security Manual*, in place of the current *Security in the Government Sector* and the *Protective Security Manual* effective from 15 December 2014;

9 **directed** all 29 Public Service departments and the New Zealand Defence Force, the New Zealand Police, the New Zealand Security Intelligence Service and the Parliamentary Counsel Office, to:

9.1 implement the PSR;

9.2 provide assurance information upon request from lead security agencies;

10 **invited** the Speaker of the House to direct the Office of the Clerk of the House of Representatives and the Parliamentary Service to:

10.1 implement the PSR;

10.2 provide assurance information upon request from lead security agencies;

11 **invited** the Minister of Finance to write to the Board of the Reserve Bank, encouraging the Board to ask the Reserve Bank to:

11.1 implement the PSR;

11.2 provide assurance information upon request from lead security agencies;

12 **invited** the Attorney-General to write to the Chief Justice, encouraging the Chief Justice to ask the judiciary to:

12.1 implement the PSR;

12.2 provide assurance information upon request from lead security agencies;

13 **agreed** to highlight the applicability of the PSR to the wider State sector (not listed above), as well as the private sector, in public announcements;

14 **noted** that the State Services Commissioner already includes requirements to manage privacy and security in the performance expectations of Public Service Chief Executives;

15 **agreed** that, for the purposes of the *Public Records Act 2005*, the PSR has replaced fully the *Security in the Government Sector* manual;

16 **noted** that the on-going cost to advise departments on how to implement the PSR will be funded by the New Zealand Intelligence Community as the PSR is a top priority in the New Zealand Intelligence Community's current Strategy, Capability and Resources Review;

17 **noted** that individual departments are expected to consider the implementation costs of the PSR within their Four Year Plans;

18 **noted** that the PSR will need to evolve to keep pace with changing threats, emerging security issues and other policy requirements;

19 **directed** lead security agencies, in consultation with the Security Intelligence Board, the Government Chief Privacy Officer and the Government Chief Information Officer, to update the PSR as required, with particularly significant changes referred back to relevant Ministers.

Secretary of the Cabinet

Reference: CAB Min (14) 39/3, SEC Min (14) 17/1

Distribution: (see over)

Distribution:
All Ministers
All Chief Executives
Speaker of the House
Clerk of the House
General Manager, Parliamentary Service
Controller and Auditor-General
Privacy Commissioner