Stats NZ
Tatauranga Aotearoa

Information privacy, security, and confidentiality policy

New Zealand Government

Citation
Stats NZ (2017). *Information privacy, security, and confidentiality policy*. Retrieved from www.stats.govt.nz.

ISBN 978-0-908350-74-2 (online)

Published in May 2017
Stats NZ Tatauranga Aotearoa
Wellington, New Zealand

Contact
Stats NZ Information Centre: info@stats.govt.nz
Phone toll-free 0508 525 525
Phone international +64 4 931 4600

www.stats.govt.nz

Contents

Context

Stats NZ's vision is to 'unleash the power of data to change lives'.

Our goals are to:

- double the value of the data provided by us to New Zealand by 2018
- create a tenfold increase in value of data provided by 2030.

Public willingness to provide data and information is central to achieving our goals, and is enabled by the high level of trust and confidence in the way we manage and secure this information. We must be mindful of public expectations about privacy, security, and confidentiality in order to maintain this critical level of trust and confidence.

We are committed to ensuring all our policies and processes (and the technology we use to support our processes) not only comply with all relevant legislation and statistical principles and protocols, but also meet public expectations, and are effectively implemented. This commitment covers our policies and processes for collecting, using, storing, keeping safe, and disposing personal and other confidential information.

To achieve this we aim to get maximum benefit from the data and information by:

- making our data and information easily accessible in line with the Government's Open Data declaration but restricting access where it is necessary and responsible to do so
- sharing data and information as freely as legislation permits, while carefully considering public expectations, commitments made at the time of collection about how the data and information would be used, and always endeavouring to protect against potential harm.

Policy objectives

The objectives of the *Information privacy, security, and confidentiality policy* are to clearly:

- define accountabilities within Stats NZ for managing information privacy, security, and confidentiality
- set out the guiding principles by which staff should make decisions regarding the privacy, security, and confidentiality of data and information they deal with as part of their job
- define Stats NZ's approach to sharing data and information.

Definitions

anonymised
Term most commonly used to refer to data from which direct identifiers have been removed (de-identified data) but is sometimes used to refer to confidentialised data. It is not a term used in this policy.

availability
Ensuring authorised users, including staff, contractors, and researchers, can access data and information for authorised purposes at the time they need to do so.

confidential information
Data and information about a person, household, iwi, or organisation that we should not disclose

to people who are not authorised to have access to it. Confidential information may be obtained from respondents, other organisations, customers, staff, or other people we deal with. Confidential information also includes embargoed releases and Stats NZ operational information that is not already publicly available.

Note: 'confidential' is a classification used by the New Zealand Government in its classification system for information pertaining to national security. Stats NZ does not hold or store any information classified confidential or any other information pertaining to national security, therefore we use the common English definition of confidential. For further information about the government information classification system, see Protective Security Requirements.

confidentialisation
The statistical methods used to protect against confidential information being disclosed to people who are not authorised to have access to it, in a way that could identify an individual, household or organisation. The statistical methods used provide a level of protection against identification that cannot be obtained from de-identification.

confidentiality
The protection of information provided by people and organisations to us and ensuring it is not disclosed or made available to people or organisations who are not authorised to access it. Authorisation should ideally be given by the person providing the information, but may also be through legislation.

data integration
The linking of data about the same person or organisation (or unit) from two or more unit record datasets, originally collected for different purposes.

de-identification
The process of removing information from microdata to reduce risk of spontaneous recognition. It typically includes removing names, exact dates of birth or death, and exact addresses.

information security
The measures put in place to protect against data and information being disclosed to unauthorised people or organisations, and to ensure appropriate availability and integrity of information.

Integrated Data Infrastructure (IDI)
Database containing de-identified people-centred microdata from a range of government agencies, Stats NZ surveys and non-government organisations.

integrity
Assurance about the accuracy and consistency of data and information and that it is authentic and complete. It includes assurance that data and information has been properly created and has not been tampered with, damaged, or subject to accidental or unauthorised changes.

Longitudinal Business Database (LBD)
Database containing microdata about businesses from Stats NZ surveys and a range of administrative data sources.

microdata
Data about individual people, organisations, households, or other units in a population.

personal information
Data and information about a person that we should not disclose to people who are not authorised to have access to it. It is a subset of confidential information.

privacy
The individual's rights relating to control of the provision, use, and disclosure of information about themselves, commonly called their personal information.

Principles

These are the eight guiding principles by which staff should make decision on information privacy, security, and confidentiality.

Ensuring privacy, security, and confidentiality

- Embed privacy, security, and confidentiality considerations in the early stages of design of systems, technologies, and processes for management of data and information (privacy and security by design).
- Design secure systems and processes to ensure we manage confidential information securely, and restrict access to approved users, both internal and external to Stats NZ, and for authorised uses.
- Before releasing information, use confidentialisation procedures, appropriate to the identified risks, to protect against unauthorised disclosure of confidential information by any reasonably foreseeable means.
- Before giving access to approved researchers, de-identify microdata to minimise the possibility of spontaneous recognition of an individual, household, or organisation.
- When disposing of confidential information, use secure destruction methods.

Open by default

- Share the data and information we manage as openly as we are permitted by legislation, while also carefully considering:
    - commitments made at the time of collection about how the information would be used
    - potential harm to individuals, households, iwi, and organisations
    - public expectations.
- Look for opportunities to collect, integrate, and use data and information to benefit New Zealand.
- Seek to maximise the value derived from the data and information we collect.
- Work with customers and suppliers to understand their needs, and aim to meet those needs, while protecting data and information from unauthorised disclosure.

Use of personal and other confidential information

- Inform people about how the data and information they provide will be used.
- Only permit use of confidential information for authorised purposes.
- Provide people and organisations with access to data and information we hold about them, provided we are able to readily access it, and we can be certain the data or information belongs to the person requesting it.
- When appropriate, correct data or information if a request for correction is made.
- Make reasonable efforts, appropriate to the intended use, to ensure the accuracy of the data and information before we use it.
- Only retain confidential information beyond the original purpose if there is long term statistical or research value in doing so.

Protecting our social licence

- Proactively seek to understand people's views on sensitivity of data and information we ask for, and understand the intrusiveness of collection processes, before deciding what to ask for, and how we use it.
- Be open and transparent about the data and information we collect and how we use it to benefit New Zealand.
- Public expectations and commitments made at the time of collection are a key consideration when we decide on the measures we use to protect confidential information from unauthorised disclosure.

Ensuring availability and integrity

- Our security processes should ensure the availability of the data and information we manage, enabling access by authorised users when required.
- Protect the integrity of the data and information we manage by implementing security measures to ensure that no unauthorised changes are made to it.
- Ensure data and information is fit for purpose before releasing it.

Managing risk

- Comply with all relevant legislative and regulatory obligations, including the Statistics Act 1975, the Privacy Act 1993, the Protective Security Requirements (PSR), and the New Zealand Information Security Manual (NZISM).
- Proactively identify and manage risk, basing our investment in information security controls on a risk assessment of our data and information and environment, and in alignment with our defined risk tolerances.
- When considering the risk associated with the release of data and information, consider potential harm to people or organisations, even if they are not able to be identified from the released information.

- Undertake a risk assessment for any proposal to change the way confidential information is managed, including a privacy and confidentiality impact assessment, to ensure we protect our data and information against unauthorised disclosure.

Sharing accountability

- Understand that everyone at Stats NZ has a role to play in safeguarding the privacy, security, and confidentiality of information.
- Ensure that everyone understands their responsibilities and the policies and procedures they are required to follow in their role.

Managing breaches

- Have procedures in place to manage breaches, incidents, and near misses.
- Report breaches, incidents, and near misses as soon as possible after detection.
- In the event of a breach, we take immediate action to contain the breach and minimise any resultant harm.

Responsibilities

Here is a summary of who is responsible for what in when applying the Information privacy, security, and confidentiality policy.

All Stats NZ staff, secondees, and contractors

- Understand the principles, policies, and procedures relating to the security and management of confidential information.
- Apply these as appropriate to their role.
- Report breaches, incidents, and near misses to the security and privacy teams.

Chief digital officer

- Fulfil the role of Chief Information Security Officer (CISO) as defined in the New Zealand Information Security Manual (GCSB, 2016).
- Develop a security strategy and security risk management programme.
- Maintain appropriate security measures to protect the information gathered, stored, and transmitted by Stats NZ.
- Manage and maintain organisation-wide information security policies.
- Manage and maintain certification and accreditation processes.
- Act as an escalation point on security-related matters.

Chief methodologist

- Manage and maintain policies and standards relating to statistical confidentialisation.
- Approve confidentialisation and/or de-identification procedures before information is released by subject matter areas.
- Assist in managing confidentialisation-related breaches.

- Provide advice and training to subject matter areas on confidentialisation methods and practice.
- Provide confidentialisation advice to partner organisations.

Chief people officer

- Ensure that staff information is held securely with access limited only to those staff who need access for HR management purposes.
- Ensure Privacy and confidentiality policies and guidelines are applied to management of staff information.

Chief privacy officer

- Maintain and manage the information privacy, security, and confidentiality policy, and any other related policies.
- Act as final escalation point on privacy and other confidentiality-related matters.

Chief security officer

- Act as final escalation point on security-related matters.

Deputy government statistician

- Approve data integration that only uses data collected directly by Stats NZ.

Government statistician

- Approve data integration proposals and escalated microdata access applications.
- Approve use of any exemptions under clauses 37A to 37F of the Statistics Act 1975 or delegating approval authority.

Information Privacy, Security and Confidentiality (IPSaC) Governance Group

- Provide governance oversight of privacy, security, confidentiality policies.
- Agree policy implementation work programmes.
- Drive implementation of the work programmes.

Manager and data custodian responsible for releasing data

- Undertake risk assessment, specify risks to be mitigated, and collaborate with Statistical Methods and data specialists to determine appropriate confidentialisation and de-identification techniques. Gain the approval of the Chief Methodologist for application of those techniques.
- Ensure analysts and researchers in their area are trained in how to apply the approved confidentialisation and/or de-identification procedures and that these procedures are applied to information prior to release.

Manager, information management

- Advise and provide education about correct management, retention, and disposal of confidential information in accordance with the Public Records Act 2005 and approved disposal authorisations.

Manager, Integrated Data Infrastructure (IDI) system

- Develop and apply guidelines and processes for data integration in the Integrated Data Infrastructure (IDI) system and assess IDI integrations for approval.

Manager, microdata access

- Develop and apply processes for assessing research and researchers to determine whether researchers and projects should be recommended for approval, and ensure requirements of the Microdata Guidelines are carried out.

Respondent advocate

- Provide a respondent perspective when policies and procedures relating to privacy and confidentiality are developed and implemented.

Security manager

- Fulfil the role of information technology security manager (ITSM) as defined in the New Zealand Information Security Manual (GCSB, 2016).
- Provide leadership, advice, and consultation on security related issues.
- Manage the implementation of security measures.
- Lead the management of security breaches and incidents.
- Lead security education and awareness activities.

Senior advisor, strategy, performance and privacy

- Design and implement approaches to implement the information privacy, security, and confidentiality policy, including education and awareness activities.
- Lead management of privacy-related breaches and incidents.
- Lead management of confidentiality-related breaches and incidents.
- Provide leadership, advice, and consultation on privacy and confidentiality related issues, including guidance on privacy and confidentiality impact assessments.
- Consult with the Office of the Privacy Commissioner when required.

The Confidentiality Network

- Provide support, advice, and build capability across Statistical Methods, Stats NZ, and the Official Statistics System in confidentiality methodologies and practices.

Related documents

Guidelines and procedures

Statistics NZ (2009). *Methodological standard for confidentiality standard for microdata access*. Available from senior advisor, strategy performance and privacy, email: info@stats.govt.nz.

Statistics NZ (2016). *Brief privacy and confidentiality impact analysis template*. Available from senior advisor, strategy, performance and privacy, email: info@stats.govt.nz.

Statistics NZ (2016). *Full privacy and confidentiality impact assessment template*. Available from senior advisor, strategy, performance and privacy, email: info@stats.govt.nz.

Statistics NZ (2016). *Privacy and confidentiality impact assessment guidance*. Available from senior advisor, Strategy Performance and Privacy, email: info@stats.govt.nz.

Statistics NZ (2016). *Privacy, security, and confidentiality incident procedures*. Available from security and privacy teams, email: info@stats.govt.nz.

Stats NZ (2017). Data integration guidelines. Available from www.stats.govt.nz.

Stats NZ (2017). Microdata access guidelines. Available from www.stats.govt.nz.

Stats NZ (2017). Privacy and confidentiality guidelines. Available from www.stats.govt.nz.

Other documents

Government Communications Security Bureau (2016). New Zealand information security manual (NZISM). Available from www.gcsb.govt.nz.

Protective security requirements. Available from www.protectivesecurity.govt.nz.

Statistics NZ (nd). *Our privacy commitment* (poster). Available from Stats NZ, email: info@stats.govt.nz.

Statistics NZ (nd). Security policies and standards. Available from Stats NZ, email: info@stats.govt.nz.

Statistics NZ (2007). Principles and protocols for producers of Tier 1 Statistics. Available from www.stats.govt.nz.

Statistics NZ (2013). *Information and data management policy*. Available from Stats NZ, email: info@stats.govt.nz.

United Nations (2014). Fundamental principles for official statistics (Principle 6). Available from https://unstats.un.org.

Legislation

Official Information Act 1982. Available from www.legislation.govt.nz.

Privacy Act 1993. Available from www.legislation.govt.nz.

Public Records Act 2005. Available from www.legislation.govt.nz.

Statistics Act 1975. Available from www.legislation.govt.nz.

Owner and review

The chair of the Information Privacy, Security and Confidentiality Governance Group (IPSaC) is the owner of *Information privacy, security, and confidentiality policy*. This policy will be reviewed annually.