INFORMATION PRACTICE

Managing our information in accordance with our principles, best practices and obligations

SHIFTS

- **Stewardship** – Strategic information is managed as an asset an stewarded through our information management practices
- **Role** - clarity of what information SSC holds on behalf of the system

SUCCESS

- **Maturity** - SSC builds its information management practices to support both our external obligations, and our internal business requirements in the most efficient and effective way.

INFORMATION MANAGEMENT

Ensuring SSC has all the information it requires to meet its needs, by identifying, collection and storing data

SHIFTS

- **Infrastructure** - SSC developed standardised systems (both technological and human processes)
- **Map –** good understanding all our strategic information assets
- **Commissioning** – SSC makes good information investments
- **Integration** – where practicable our information assets are integrated

SUCCESS

- **Future proofed** - SSC builds our systems in a co-ordinated way with one eye to our future
- **Errors** – reduce errors through good data management practices
- **Cost effective –** System needs are met within our resource constraints

INFORMATION IS AN ASSET

Information should be seen as an asset of SSC so that it is managed and used to realise its full value

INFORMATION INTO INSIGHT

Information supports SSC to monitor, design and evaluate the performance of the State Sector

INFORMATION IS WELL MANAGED

Information is managed efficiently and can be trusted as being accurate.

INFORMATION IS PROTECTED & OPEN

Information held by SSC should be proactively shared across SSC and with the Public *unless there are grounds for refusal, such as for personal, confidential or classified information*

SHIFTS

- **Flow**- we understand who the customer(s) is/are for all our information
- **Visualisation** – information is presented in a way that makes it useable and easily understood for our customers

SUCCESS

- **Sharing** – our information is open, unless withheld due to privacy and security.

Understanding who needs our information both internally and externally and sharing it with them

INFORMATION SHARING

SHIFTS

- **Capability** - SSC understands and builds the capability to analyse our information
- **Research programme** - a research and evaluation programme is established and maintained to analyse critical system risks and opportunities

SUCCESS

- **Insights** - our information is used to derive insights on how to improve performance of the system, agencies and chief executives or any form of customer segmentation

Using our Information to draw actionable insight

INFORMATION ANALYTICS

SSC INFORMATION ROLES AND RESPONSIBILITIES

ROLE	DESCRIPTION	KEY RESPONSIBILITIES
SENIOR DATA STEWARD	A role held by a tier-2 manager sitting on SMT (currently the EMPG CE) who has oversight over information management and release across SSC on behalf of the Commissioner.	• Manages risks around high value public information releases • Reviews information management and release policies • Reviews and sponsors new strategic information projects • Communicate and promote the value of information
SMT	SMT are the Governance group who uphold the principles of the Information Strategy in relation to decisions around managing SSC's strategic information.	• Approves SSC's information management and release policies • Makes investment decisions around improving our information resources, including commissioning work through collaboration hub processes • Approval over what is 'Strategic' information (and therefore subject to all controls)
DATA OWNER	Has legal rights over the information, including copyright ownership. For SSC, as a department, all information developed internally or acquired via legislative provision, are owned by the Crown. Information supplied by holders of external copyright remains in their ownership regardless of the usage licence acquired by SSC. Ownership of an information system does not equate to ownership of the information.	• Provides permission for the use and reuse of their information, either through written consent, or the use of creative common licences or similar copyright
DATA STEWARD	Stewardship duties belong to business units within SSC that are most concerned with a particular information resource. This is a business function, not a technical one.	• Adheres to the information management and release policies • Establishes information requirements and supports procurement of information resources. • Sets expectations for how information is to be managed, including security, privacy and access settings • Ensures information is used in accordance with the purposes for which it was collected, including adherence to copyright • Approval and contribution to open data releases
DATA CUSTODIAN	The technical specialists who develop and administer information management practices. The Strategic Information Team is generally the custodian on behalf of SSC, although external service providers managed via contract (e.g. TMIS) can also be the data custodian.	• Develops and administers the Information Strategy and information and release policies • Advises on, and monitors the use of, SSC's information management and release policies • Sources data and metadata, in terms of content, quality, and conformance with standards and the Public Records Act, 2005 • Ensures that appropriate Service Level Agreements are in place with platform and data services support providers, including CASS IT • Ensures expectations and rules set by the Data Steward are appropriately implemented • Co–ordinates release of data to agencies to drive performance improvement and the public under open data requirements. • Supports information creation through day-to-day service provision and maintenance of information systems • Support SMT in its role, in particular in assessment of investment in strategic information
SSC DATA USER	SSC staff who analyse information, as part of their day-to-day work, to generate actionable insights.	• Knows their responsibilities with information as set out in SSC's information protocols • Must adhere to the privacy and security rules and guidance set out in SSC's information protocols, in particular when externally releasing information • Must adhere to copyright obligations
EXTERNAL DATA USER	Those looking to SSC information to provide them insights into the State Sector.	• Must adhere to Crown copyright obligations

SSC INFORMATION MANAGEMENT PROTOCOLS

PROTOCOLS	PRACTICES	RESOURCES
WE EMBED OUR INFORMATION ROLES AND RESPONSIBILITIES	• Information is an important asset with appropriate governance structures • Information sources each have a steward responsible for life-cycle management • All staff know their responsibilities with information • These responsibilities also apply to external researchers given access to SSC data	• INFORMATION ROLES AND RESPONSIBILITIES
WE SECURE THE CONFIDENTIALITY AND PRIVACY OF OUR INFORMATION	• Legal and ethical obligations around managing information are adhered to • The permissions we have to use data are understood • Security practices are built into our processes and infrastructure • Privacy or security breaches are managed openly and quickly, recognising the seriousness of maintaining confidentiality	• PRIVACY POLICY • CONFIDENTIALITY GUIDELINES
WE INVEST WISELY IN OUR INFORMATION RESOURCE	• All data that is collected has a clear use and its value is understood • Information is actively used, and then archived, to get full value from it • Data is appropriately and efficiently sourced • Information infrastructure is invested in to enhance the value of our data	• INFORMATION REGISTER • COLLECTION GUIDELINES
WE ASSURE OUR INFORMATION QUALITY	• There is a culture of professionalism and good practice • Information meets the needs of users, within available resources • Information is accurate • Information is timely enough to be of value to users • Information is consistent • Methods used to produce information are understood and documented	
WE SHARE AN INFORMATION LANGUAGE	• Common information standards are used to manage SSC information • SSC uses national and international information standards where possible • SSC promotes common information standards across the system	• INFORMATION REGISTER
WE USE OUR INFORMATION WISELY	• Information infrastructure assists with turning data into insight • Processes get the right information to the right people at the right time • Published information is presented clearly and supported by analysis • Published information is open and accessible • Published information is understandable • Significant errors in published information are corrected quickly	• RELEASE GUIDELINES • DECLARATION ON OPEN AND TRANSPARENT GOVERNMENT

State Services Commission (SSC)
Information Management Protocols

A principal of SSC's Information Strategy is to manage our strategic information[1] in accordance with our principles, best practices and obligations.

The six information protocols are:

1. We embed our information roles and responsibilities
2. We protect the confidentiality, privacy and security of our information
3. We invest wisely in our information resources
4. We assure our information quality
5. We share an information language
6. We use our information wisely

Each protocol consists of:

- Practices: short statements to be used by SCC teams to guide behaviour around information.
- Resources: links to more in-depth material to support SSC teams.

The information protocols draw, where appropriate, on Statistics New Zealand's *Principles and Protocols for Producers of Tier 1 Statistics* which can be found at http://www.statisphere.govt.nz.

[1] Strategic information is defined in the Information Management and Release Policy document.

PROTOCOL 1: We embed our information roles and responsibilities

1.1 Our information is an important asset with appropriate governance structures

SMT have governing authority over SSC's strategic information. Key governance responsibilities include making key investment decisions and establishing the information management practices. SMT are supported by the Strategic Information team (SIT).

RESOURCE: Information Roles and Responsibilities

1.2 Information sources each have a steward responsible for life-cycle management

All data coming into SSC has a business owner, called the Data Steward. The Data Steward is ultimately responsible that the data is well managed.

The Data Steward is supported by Data Custodians. These are technical data specialists who develop and administer data management practices. Data Custodians will generally be SIT, but may be CASS IT or contracted out to external provider.

All data has a data owner that ultimately has legal rights over the information. For information, where SSC is the data owner, either information that is developed internally or acquired via legislative provision, these assets are in owned by the Crown.

RESOURCE: Information Roles and Responsibilities

1.3 All staff know their responsibilities with our information

These protocols set out the roles, responsibilities and rules for SSC staff to adhere to. All staff involved in the use of SSC strategic information are aware of their obligation to protect confidentiality and privacy, and are aware of the penalties for wrongful disclosure.

1.4 These responsibilities also apply to external researchers given access to SSC data

Bona fide researchers may be given access to anonymised individual-level SSC data to undertake statistical work that is in the public interest and subject to their ethics application. A condition of granting access is that researchers agree to follow the SSC's information management and release practices as if they were an SSC employee. A CASS approved method must be used to exchange unit record data.

A Privacy Impact Assessment should be undertaken for all major requests that involve sharing individual-level SSC data on a systematic basis with new strategic or research partner(s).

PROTOCOL 2: We secure the confidentiality and privacy of our information

2.1 Legal and ethical obligations around managing information are adhered to

The legislative and ethical obligations governing the collection, storage and release of information are built into SSC policies and information practices (SSC's Privacy Officer is responsible for ensuring SSC policies and practices conform to legislative obligations).

All staff involved in the use of SSC strategic information are aware of these obligations to protect confidentiality and privacy and the penalties for wrongful disclosure, and adhere to these obligations.

RESOURCE: Privacy Policy

2.2 The permissions we have to use data are understood

Survey respondents and data owners provide permissions for the use of their data. SSC only uses data in a way consistent with these permissions and the reason(s) for which the information is collected. Permissions and use of information is documented and stored with our information asset register. Staff need to confirm that they understand and agree to these permissions prior to getting access to some types of strategic information.

We are sure of the need for the data before asking for it. Respondents are informed of their rights and obligations in providing information. Respondents are clear why we are collecting the information and are aware of our security controls to maintain their privacy and confidentiality. The respondent's confidentiality is always strictly preserved unless they have explicitly agreed to the contrary.

2.3 Security Practices are built into our processes and infrastructure

Security practices are built into our infrastructure. SIT and CASS IT administer security practices across our business intelligence (BI) environment. Identifying information (such as name) should be removed from BI datasets or datasets provided to external researchers. Rules are established (such as minimum counts) to ensure identifying information is suppressed before aggregated results are released outside SSC. SIT can help with establishing, and checking the implementation, of these rules.

Security practices include explicitly setting out the rules for access to private and confidential information by a user. It is the data steward, who sets those rules, which must be documented. The data steward also needs to ensure users acknowledge the rules that they can operate within, including their responsibilities to maintain privacy and confidentiality, including keeping an audit trail.

2.4 Privacy or security breaches are managed openly and quickly, recognising the seriousness of maintaining confidentiality

As per our Privacy Policy, the Privacy Officer is notified immediately of any potential privacy breaches.

PROTOCOL 3: We invest wisely in our information resources

3.1 Strategic Information is invested in to enhance the value of our data

When assessing whether to invest in a new information collection, we must first consider if it meets the definition of strategic information.

If the new collection does meet the criteria, SSC teams should talk to SIT who can help assess whether to invest in the information and the level of maturity based on a number of technical consideration that include value for money.

RESOURCE: Collections Guidelines

3.2 All data that is collected has a clear use and its value is understood

The value of the data we collect is understood. Data collection has clear objectives and information needs that we are attempting to address. We balance the need to collect data to inform decision making against the costs of production and the burden placed on the system.

Investment decisions are made by the SMT. Work programmes are periodically reviewed to ensure their relevance, and justify their continuation.

3.3 Information is actively used, and then archived, to get full value from it

We maximise the use and value of existing data by integrating or aligning it with administrative sources. SSC understands (through the Data Architecture) and has shared access to all our information resources to be able to get best value from the information. We share our information with the system and public so that they can derive value from it.

Business processes adhere to the CASS disposal and retention policies and rules set out in the Public Records Act 2005. In practice however, most data is retained indefinitely due to its potential research value, subject to security, confidentiality and statutory obligations.

3.4 Data is appropriately and efficiently sourced

We ask for data only once and then share internally. Similarly, Information requests to the same respondents are co-ordinated, in particular to agencies and CE's.

Existing data sources are used wherever possible and existing collection mechanisms are considered when looking to capture new data. Appropriate opportunities to reduce costs are actively sought. These include economies of scale, data integration, and methodologies and systems that use generic and/or automated processes

Data collection is designed in a supplier friendly way and with sufficient flexibility to accommodate changes in user needs. SIT can help develop and build standards for data collection, including the design of survey questionnaires.

3.5 Information infrastructure is invested in to enhance the value of our data

SSC's existing information infrastructure, referred to as the BI environment, is the enterprise solution for SSC. Where possible SSC uses this BI environment to enable better integration of data. When investing in new data collection, storage or administrative systems SSC assesses it for compatibility with the existing BI environment.

New technologies are routinely investigated to see if they would provide value to the BI environment. Where possible SSC look to link the BI

environment with other central agency partners for a whole of CASS enterprise solution.

PROTOCOL 4: We assure our information quality

4.1 There is a culture of professionalism and good practice

Analysts act with integrity, objectivity and comply with SSC's information protocols.

SSC uses good data and project management processes in the production of information. SSC invests in training and development to ensure analysts have the information skills required. SSC regularly assesses information processes and tools; seeking opportunities to implement new technologies and maintaining a culture of peer review.

4.2 Information meets the needs of users, within available resources

SSC designs new information to be relevant to users' needs, within available financial resources. SSC teams understand who the key users of their existing information are and why they use it. They consult their key users before making substantial changes to how the information is collected, managed or reported.

4.3 Information is accurate

SSC produces its information using sound data and methods. It does this by validating incoming data, and understanding or, where possible, controlling the level of error in its information (e.g. minimum counts).

Reports that will be published or ministerial briefings must have any quantitative information checked by SIT, or someone with the requisite knowledge.

4.4 Information is timely enough to be of value to users

To be relevant, information needs to be released in sufficient time to meet key users' needs. Timeliness is a decision involving trade-offs between quality and cost.

Regular publicly released information should have planned release dates.

4.5 Information is consistent

Key information results should be reported consistently (i.e. there is one version of the truth). Analysts should check to see whether information has already been reported, and if so, use the same figure. Where information is not comparable, it should be flagged as such to key users. Key users are advised of substantial changes to methods that affect consistency with previously reported information. Consistency will be facilitated through the information infrastructure (e.g. through Tableau).

4.6 Methods used to produce information are understood and documented

Understanding how information is produced sheds light on the quality of SSC's information

Both the methods and classifications used in producing the information and measures of the accuracy of the data (e.g. sample counts) should be documented. Documentation is regularly reviewed and updated. Its level of detail suits the needs of its intended audience. Documentation should be standardised across SSC where possible.

PROTOCOL 5: We share an information language

5.1 Common information standards are used to manage SSC information

SSC works to apply common frameworks, classification, derivations and metadata to ensure that information has the same meaning across the organisation and that separate datasets can be related to each other.

- Frameworks are a logical structure for organising complex information (e.g. National Accounts)
- Classifications organise data by grouping similar items into understandable categories (e.g. Australian and New Zealand Standard Classification of Occupations ANZSCO)
- Derivations are standardised ways to calculate one variable from another (e.g. gender pay gap)
- Metadata is information that helps provide context around data (e.g. response rates)

At SSC, our core framework looks at the varying dimensions of performance which can be aggregated and disaggregated between CE, agency, sector and system. These common standards will be incorporated in all new survey and administrative data collections. They should be incorporated into existing data collections during major revisions or upgrades to minimise costs.

SIT will be data custodians for information frameworks, standards, classifications. SIT will ensure that this common information language is embedded into SCC practice through Tableau and documented into the Data Architecture.

5.2 SSC uses national and international information standards where possible

To facilitate meaningful comparisons between agencies, sectors and countries, SSC information frameworks, classifications and derivations should align wherever possible with existing system, national and international standards.

SIT can advise on whether there are relevant existing information frameworks, classifications and derivations.

5.3 SSC promotes common information standards across the system

SSC works cooperatively with other agencies in the development of common information frameworks, standards, classifications and derivations.

SSC documents its common information frameworks, standards, classifications and derivations and makes them available to other agencies, and supports other agencies to use them.

PROTOCOL 6: We use our information wisely

6.1 Information infrastructure assists with turning data into insight

SSC has a package of state of art tools (Tableau, R) that can turn data into insight. The SIT team can advise on using these tools.

6.2 Processes get the right information to the right people at the right time

Information supplied meets user needs, in terms of substance and timeliness. Published information is secure before it is released (refer to the Release Guidelines). Information requests should come directly from users or should be put in writing.

RESOURCE: Release Guidelines

6.3 Published information is presented clearly and supported by analysis

SSC information is objective. Conclusions are supported by analysis.

6.4 Published information is open and accessible

SSC information meets its Open Government obligations. Anyone can freely access, use, modify, and share SSC published information, detailed information is released onto open.govt.nz. Published information is made available to all at the same time, where possible.

RESOURCE: Declaration on Open and Transparent Government

6.5 Published information is understandable

Information is presented clearly and simply, with easily understandable conclusions. This can be achieved through written commentary, maps, graphs and statistical tables. These should follow best practice so that they are easy to read and do not mislead. The decisions behind the type of commentary and analysis provided should be reasonable. Judgement is used to tailor the presentation of SSC published information to our targeted users. Information that is published for transparency purposes communicates key results in straightforward terms for the wider public.

As much detail as is reliable and practicable is made available, subject to confidentiality constraints. To encourage comparative analysis and to provide context, dissemination should include background information on metadata, trends and links to related information. Recurring information releases are delivered in consistent formats. When SSC reuses data collected by others, credit is given to the original data source.

6.6 Significant errors in published information are corrected quickly

All published errors are handled in a standard manner consistent with their significance and revised when necessary. Revisions practice is covered in the Release Guidelines.

SSC INFORMATION RELEASE PROTOCOLS

These protocols formalise governance around the public release of information from the Commission.

1 High value information is published where possible

- SSC meet's its obligation under the Declaration on Open and Transparent Government to actively release high value public information. High value public information:
  - "Is publicly-funded data, which when re-used contributes to economic, social, cultural or environmental growth, illustrates government's performance, and contributes to greater government efficiencies through improved information sharing. Public data is non-personal and unrestricted data."[1]
  - Should be determined from the public's point of view. OIA requests can help SSC identify its high value public information.
- To support this obligation, SSC follows the New Zealand Data and Information Management Principles:
  - Information is open, unless restricted by OIA or other policy.
  - The withholding provisions of the OIA are useful guidelines when considering whether to release information (see SSC's Official Information Act (OIA) Guidelines):
    - protect New Zealand's security
    - protect the privacy of natural persons
    - protect information where making it available would be likely to unreasonably prejudice a person's commercial position
    - protect information that is subject to an obligation of confidence
    - avoid prejudice to health and safety
    - maintain the constitutional conventions that protect the confidentiality of advice tendered by Ministers of the Crown and officials
    - maintain the effective conduct of public affairs through the free and frank expression of opinions
    - maintain legal professional privilege, or
    - enable a Minister or department to carry on negotiations without prejudice or disadvantage
  - Information is released proactively and readily available online

[1] https://www.ict.govt.nz/guidance-and-resources/open-government/community-sector/

- Information is free where possible
- Information is released in a form that makes it easily reusable (i.e. most detail possible, machine readable, with metadata

- To support regular publicly released information should have planned release dates scheduled in the Proactive Release Programme.
- SSC shares high value system information with agencies to support system performance.

2 Published information is well managed

- Published information has been managed under SSC's Information Management Protocols, to ensure that:
  - Published information is trusted and authoritative (i.e. accurate, relevant, timely, consistent and without bias)
  - Personal, confidential and classified information has been protected.
    - SSC's Confidentiality Guidelines provide guidance on how information privacy and security can been maintained. These are consistent with Privacy Act requirements and have been developed in consultation with Statistics NZ. The SIT can help with applying the Guidelines.
- Quantitative information is checked before release to ensure its accuracy.
  - Published information accurately describes the reality it represents. Reports that will be published or ministerial briefings need to have any quantitative information checked by someone with the requisite knowledge, and need to be discussed with SIT, if they substantially rely on quantitative information.

3 Published information is secure before release

- Access is restricted to specified individuals or agencies prior to public release. These are:
  - Those directly involved it is production
  - Ministers
  - System leaders
  - Select Committees
  - Information provided early for agency Annual Report publication timelines
  - Agencies, who provide the raw data, can access their own information along with any system benchmark information
- All others enjoy equal access to published information. It is made available to all at the same time.

4 Revisions are managed openly and transparently

- Published errors are handled in a standard manner consistent with their significance and revised when necessary. All errors in SSC published information need to be reported to the tier three manager responsible for that information. The tier three manager should classify the error as either:

  - An error that significantly alters the meaning of the previously published information. Tier two manager needs to be informed. This needs to be revised on the website as soon as possible. Users need to be identified as soon as possible.
  - Errors that do not significantly alter the meaning of the published information may be revised with the next regular information release, or if in an irregular release, when it is convenient to SSC to do so.
  - Errors that do not alter the meaning of published information and that will have very little or no impact on users. These errors can be ignored (revisions which are frequent and trivial will undermine user confidence).

- For each major information release, we publish and maintain a general statement describing SSC revision practice.
- Users should know when planned revisions are due and be aware of them as they arise. Scheduled revisions are managed systematically, pre-announced and are reflected in communication plans.
- All revisions should be accompanied by documentation which explains their nature, provides good analysis of the differences between the original and revised information and explains the effect on any previously published commentary or interpretation.

State Services Commission (SSC)
Information Collection Guidelines

These guidelines set out our practice around information collections at SSC and should be used in conjunction with the information management and release protocols and the other resources provided in this document.

1. Roles and responsibilities are adhered to

- All staff have a duty to take reasonable care of sensitive information provided to them, this can be physically, electronically or even verbally.
- SSC staff should know their responsibilities with SSC information and their obligations to protect confidentiality and privacy.
- Prior to being granted access to sensitive strategic information, staff need to acknowledge the rules set by the data steward.

2. Information is collected to meet a specific purpose

- The need for new information should be outlined with clear objectives before any data collection is implemented.
- The value of the data SSC collects is understood and weighed against the cost of collection.
- Information is collected for specific purposes and used as intended, in a way that aligns with the permissions the data owner has provided (in accordance with the SSC privacy policy and the information privacy principles of the Privacy Act 1993).
    - For current collections - if the permissions are unknown it is our responsibility to identify what the permissions are before sharing or publishing any information or analysis.
- Personal, confidential and classified information is protected and respondents understand their rights and obligations in providing information.

3. Our information is well managed

- All information strategic or non-strategic needs to be managed well.
- SSC need to determine if the information is meets the definition of strategic information.
- New strategic information collections require LT approval. SIT can help input into the decision paper for LT.
- All strategic information needs to be managed in accordance with Information Management & Release Protocols. However not all strategic information needs to be brought into the managed information environment. Data that is not built into this environment will likely be stored the document management system (iManage).
- SIT will consider incorporating a new information collection into the managed data environment based on a number of considerations. SIT may incorporate a collection into the environment if:
    - The information is ‘strategic Information’
    - The collection will be repeated regularly
    - The information could be used to link with other data sources

- SIT are unlikely to incorporate a collection into their environment if:
  - The information is corporate information
  - The information is 'strategic information' and the collection is an ad-hoc one off
  - The nature of the information is not strategic
- If the information is not strategic, SIT can still provide advice and support to ensure information is well managed.
- When investing in a new collection, storage or administrative systems, SSC and SIT need to ensure it is compatible with the current environment.
- When information needs have been defined and the collection is approved a data custodian from SIT will work closely with the business owner (or data steward) throughout the project. For more information about these terms see section 1.2 of the Information Management Protocols.

4. New collections are well designed

- SSC teams should come talk to SIT if the need for new information has been identified
- SSC need to manage information collections well – this means information is managed efficiently, effectively and can be trusted as being accurate.
  - Designing information collections is the first steps in our process and it is important SSC teams talk to SIT at this stage so SIT can help design and develop tools that are fit for purpose.
- SIT will approach SSC teams to review their information needs every two years, including reassessing current collections.

5. Information collections are implemented in a respondent-friendly manner

- SSC teams should talk to SIT before asking for information from agencies or individuals as the information may already be captured (and we should never ask for the same information more than once).
- If SIT do not have the required information, we need to consider:
  - The individual providing the data and how much work is involved in producing it. The information should be readily accessible to the respondent.
    - Data should always be collected from the most appropriate source.
    - It may be more efficient and less intrusive to collect the information through a third party.
  - The best tool to capture the information in a respondent-friendly manner (e.g. Excel, survey monkey or other option)
  - How the information will be used and the questions it will answer, to ensure the right data is captured.
  - Respondent-friendly language is used and statistical jargon is avoided – SIT can provide advice on questionnaire wording.
  - Any information standards we use – SIT can provide advice on current standards, classifications and derivations.
  - How frequently we should ask for the information.
    - The data needs to be relevant enough to meet the information needs, however the frequency of a data collection should be weighed with the burden placed on respondents and cost of collecting the data.

6. Appropriate collection channels are used and collected data is validated

- Identifying the right channel to collect data
  - The transfer of data needs to take place in a secure manner.
  - Minimising the burden placed on respondents, should be considered when determining the right channel.
- The channels available include:
  - Less mature channels:
    - Electronically – Email attachment.
    - Physical Transfer – USB drives, Iron Keys, CDs
  - If the information is sensitive, additional security measures should be put in place such as password-protected files.
- More mature channels:
  - Secure portals that require data submission:
    - Survey Monkey
    - Next Cloud
    - CFISnet
- Most mature channel:
  - Accessible Systems (API)
- More information about each of these channels can be found in Appendix 1 at the end of these information collection procedures.
- New tools for collecting information should be tested thoroughly before implementation to ensure they can work within our managed environment and that any bugs are found and fixed.

7. Collection Maturity Model

Less Mature	More Mature	Most Mature
Manual input and checking of Raw Data		Automated data collection & validation
Manual integration with other data sources for analysis		Data is integrated with other data sources on collection
Raw data exists in multiple places, no single source of truth	Central source of truth, protections against data loss	Data stored in database
Calculations hard to trace back and repeat	Clear transparent calculation processes	Automated calculations
Data collection is owned by the business unit	Data collection is centralised	Data collection is automated, minimal maintenance required

- Criteria to assist in vehicle selection:
  - Repetitive – is the data collection going to be repeated? If yes, more mature methods are desirable.

- Content likeliness to change – will content potentially substantially change? If yes, more mature methods provide less value.
- Analysis complexity – is analysis time consuming and / or difficult to understand? If yes, more mature methods are desirable.
- Security – is data sensitive? If yes, more mature methods are desirable.
- Turnaround time – Is speed of collection and analysis important? If yes, more mature methods are desirable.

- Validating the data we collect:
  - When information is collected the data needs to be validated to ensure:
    - The data has been collected as intended and is consistent with other instances of the collection (if the information is collected regularly).
    - Any erroneous data is amended in a consistent way.
- To validate the data:
  - Build in validation rules.
  - Check the data has been collected correctly (the correct template and data types).
  - Check for outliers in the first instance – Any specific values that do not look correct should be checked with the data provider, if the value is incorrect, the data needs to be updated.
  - Additional checks should be completed as the information is analysed such as:
    - Changes over time – if there are large differences this may be due to an error in the data; otherwise determine the reasons for the change.
    - Large differences compared with other respondents.

It is also important to note if any information is going to be released to the public (regardless of where the collection is managed) needs to be checked and the Information Release Guidelines should be adhered to. – SIT complete checks to ensure the information we release is accurate and confidential.

8. Collections are reviewed regularly:

- Regular collections are reviewed periodically to establish whether:
  - we can improve the method of collection
  - the information is still necessary
  - other appropriate data sources have become available
  - the views of respondents and users of data are being taken into account
  - variables are used effectively and that only necessary information is collected

Related Guidance:

Information Strategy Diagram

Information Management & Release Policy

Information Management Protocols

Information Release Guidelines

Information Confidentiality Guidelines

Information Roles and Responsibilities

SSC Privacy Policy

SSC OIA Guidelines

Appendix 1. Collection Channels

More mature channels:

- Secure portals that require data submission:
    - Survey Monkey - Surveys are created in Survey Monkey and the data captured from respondents is securely stored on the Survey Monkey server. The data is owned and administered by the survey creator, however Survey Monkey do have the right to access the survey data to provide the survey creator and respondents support. Survey Monkey also have the right to share the information you capture in some cases (such as if they obtain your consent or if they aggregate or de-identify the information).

      Survey Monkey allows the survey creator to control who completes the survey. Survey Monkey is a good option for collecting information from a number of individuals based on specific questions identified to answer an information need. This option would be preferred to collecting the data electronically or physically from each individual and collating the responses together which would be very time consuming.
    - Next Cloud - Next cloud can be used for sharing information by loading the data into next cloud and setting up access for users you want to share the information with. The users' username and password should be sent via email independently of the link to the next cloud file.
    - CFISnet - CFISnet is used to collect confidential data in a secure manner. The data is uploaded into a CASS managed database once the sender has logged in to RealMe to verify their identity for security purposes. This option has been set up for regular confidential data collection.

      CFISnet is used to collect the HRC data and is the right tool to collect this data because it is a secure file transfer process for large sensitive files.

Most mature channel:

- Accessible Systems
    - These are systems that don't require manual steps by users to submit data e.g. APIs that developers can access programmatically. Examples of this include the SAP API for Talent Exchange data, the DIA Govt. A-Z directory API for agency and ministerial contact information.

  Channels such as CFISnet and APIs would only be used for Strategic Information and managed by SIT.

Information Release Confidentiality Guidelines

The release guidelines state that Te Kawa Mataaho Public Service Commission (TKM) should **release high value** information where possible, while also protecting personal information. These guidelines make this possible by allowing as much high value information available for release, while ensuring that it is:

- not in a form that could reasonably expected to identity an individual, or
- at a level of aggregation where the information is still informative.

The guidelines are consistent with Privacy Act requirements and were developed in consultation with Stats NZ (see Stats NZ's Data Confidentiality report for more detail).

The guidelines apply to:

- all strategic information
- any statistical information that contains private or confidential information.

1. Roles and responsibilities are adhered to

- All staff have a duty to take reasonable care of sensitive information provided to them, this can be physically, electronically or even verbally.
- TKM staff should know their responsibilities with TKM information and their obligations to protect confidentiality and privacy.
- Prior to being granted access to sensitive strategic information, staff need to acknowledge the rules set by the data steward.

2. Use of confidential data within TKM

- Even if information is not going to be disclosed publicly, or external to TKM, privacy and confidentiality should be maintained.
- Information should be provided to users of the information at the highest level of aggregation, and/or anonymised, while still being informative for the purposes of the user.
- When providing information to users that is private or confidential in nature, you should inform the user of this, and if necessary ensure that they know their roles and responsibilities.

3. Information release rules

- All users of information should follow the release rules provided in Tables 1 and 2 below. The release rules provide statistical advice on aggregation, suppression and counts.
- Information release rules apply to all personal information, which are outlined in table 3.
- TKM can choose, in the following circumstances, not to apply the rules:
    - When suppling information back to the original supplier of the data. For example, agency workforce information back to the HR team of that agency.

- If information is already public or can be easily ascertained by a member of the public. For example, the gender of senior leadership team members.
- When reporting information that is organisational, rather than personal, in nature. For example, counts at an agency by, job title or occupation, level. See table 3 for examples of personal information.

- ***Note*** Stats NZ advises that gender pay gaps are not statistically robust for groups of fewer than 20 men and 20 women. Gender pay gaps for smaller groups can be released, if they meet the other rules in these guidelines and the release is accompanied by reference to this information not being statistically robust according to Stats NZ.
- Note that Te Kawa Mataaho has an agreement with GCSB and NZSIS to not release any information collected in the Workforce Data, beyond that published in these three tables.

Table 1 – TKM Information Release Rules

	Counts (e.g. Headcount, FTEs)	**Magnitudes (e.g. Salary, Sick Leave) Means & totals**	**Magnitudes (e.g. Salary, Sick Leave) Medians & percentiles**
Full coverage (e.g. Workforce Data collection)	Suppress cells with counts below '4' (this takes the possibility of collusion into account). Make them appear like cells with zero counts (i.e. either with a zero or by leaving blank). **Or** Apply random rounding to base 3 by using this workbook. Note any use of random rounding. Totals and percentages should be calculated using rounded numbers. **Additional rule if needed** Apply both rules if many tables are being produced that may mean values can be determined by looking across tables or a highly sensitive variable is involved (e.g. income).	Suppress cells with counts below '4' (this takes the possibility of collusion into account). Make them appear like cells with zero counts (i.e. either with a zero or by leaving blank). Round magnitude values to an appropriate level. For example, round average salary to the nearest $100, round average tenure, age and sick leave to one decimal place. Percentages should be calculated using rounded numbers. **Additional rule if needed** Suppress cells with counts below '10' in the following circumstances: The use of multiple variables (e.g. occupation by department) or detailed variables (e, g. occupation at very detailed levels) means the risk of identifying an individual's information is high and the value is highly sensitive (e.g. income).	Apply table 2.

Sample surveys (e.g. Kiwis Count)	Kiwis Count rules are about ensuring robustness of results, rather than confidentiality. The small size of the Kiwis Count survey means that it is very unlikely that an individual can be identified. Kiwis Count unit record data is published on the TKM website after detailed regional council information is removed. Results for questions with unweighted sample counts of less than 25 are suppressed with a 's' due to potentially high margins of error. Results for questions with unweighted sample counts of less than 50 (i.e. those answered by less than 50 people) are released but are flagged that they may be subject to high margins of error due to small samples.

Table 2 – TKM Information Release Rules for Magnitude Medians and Percentiles

Percentile	Minimum count needed overall
1st	500
5th	100
10th	50
25th	20
50th (median)	10
75th	20
90th	50
95th	100
99th	500

Table 3 – Workforce Data person-level variables: Personal Information?

Variable	Personal information?
Gender	No for Male. Female (personal, but not private) Yes for Another Gender
Ethnicity	Yes
Date of Birth / Age	Yes
Occupation / Job Title	No
Department / Business Unit	No
Status – Current employee / Seconded / Previous employee	No
Status – On Parental Leave / On other LWOP	Yes
Salary	Yes
Full-time Equivalent / Part-time	No
Contract Term (Permanent or fixed-term)	No
Tenure / Start or end date	No
Termination reason	Yes
Region	No
Management tier	No
Sick and domestic leave taken	Yes