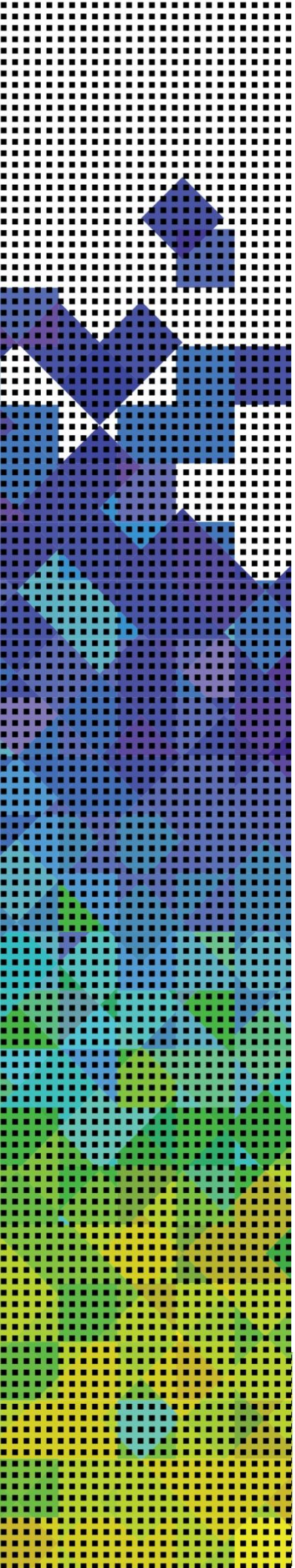

Government Information Sharing Policy

Sultanate of Oman
Information Technology Authority

e.oman

Policy:

1. Introduction

1.1. This document sets out the policies for sharing information among the agencies of the Sultanate of Oman and supports the implementation of standards and best practices outlined in OeGAF Information Reference Model.

1.2. Agencies that are involved in providing services to the public have a responsibility to ensure that their use of personal data is lawful, properly controlled and that an individual's rights are respected. The key challenge in information sharing is in finding the right balance between the need to share data to provide quality services and the need to ensure protection of confidentiality.

1.3. While this document consists of the principles and policies for information sharing, the procedures and templates that support the policies are to be referred to the OeGAF Information Reference Model and the OeGAF Solution Reference Model.

2. Aims of the Policy

2.1. The policy outlines the principles and standards of expected conduct and practice of the agencies and their staff and applies to all types of sharable data. It establishes the organisation's intentions and commitment to data sharing and promotes good practice when sharing data.

2.2. It aims to support necessary data sharing between organisations to facilitate the delivery of better services to citizens/residents and also to enable eTransformation initiatives of the Nation and includes:

- the general principles of data sharing
- the legal basis for sharing data
- the common purposes for holding and sharing data
- the responsibilities of agencies involved in information sharing

2.3. It is expected that specific information sharing arrangements between some agencies will be developed separately. These will specify precisely what data is to be shared, how it will be shared and stored and to whom that data will be given for a particular area of activity. Responsibility for producing these arrangements rests with the agencies that are involved in an information sharing requirement. In certain cases, ITA has signed a master agreement with the source agency such as in the case of ROP. For basic information, government entities can interact directly with ITA.

3. Coverage of the Policy

This policy applies to all Oman's government agencies which interact with the public that includes citizens, residents and commercial establishments. As part of the eGovernment Transformation Plan, government agencies have to provide useful eServices and information to the public. As there are many data that have been collected and managed by various government agencies and to improve the management of public data and eServices, it is extremely important that public data to be shared among the government agencies. All types of data sharing is covered under this policy

4. Legal Responsibility for Sharing Information

- Agencies need to adhere to prevalent laws and regulations such as Royal Decree 118/2011 and eTransformation Mandate from the Cabinet.
- Any exceptional reason for not sharing data needs to be discussed with the Integration and Shared Services Department of ITA along with adequate justification for an appropriate decision.

5. Purposes for Data Sharing

5.1. Data shall only be shared for lawful purposes. The specific range of purposes will be identified within the separate and specific information sharing arrangements between the agencies.

5.2. Practitioners should make use of data in an anonymised manner where such data will suffice.

5.3. Agencies should ensure that data is shared on the principle of 'need to know' basis. This means that staff will have access to data only if they need this for the fulfilment of their respective role. It may not be necessary to disclose all data and only such data that is relevant for the purpose for which it is disclosed should be passed under the information sharing agreement.

5.4. As part of evaluation of any information sharing request, agencies should consider the risks to individuals in the collection, use, sharing and disclosure of personal information.

6. Information Sharing Principles

6.1. The following are guiding principles for systematic data sharing:

- The potential benefits and risks to individuals and/or society of sharing or not sharing should be assessed.
- Records must be kept of decisions and the reasons for it - whether it is to share data or not. If the decision is to share, then it must be recorded as to what has been shared, with whom and for what purpose.
- It must be ensured that the data that is shared is necessary for the purpose for which it is being shared, is shared only with those people who need to have it? Is it accurate and up-to-date? Is it shared in a timely fashion? And is it shared securely?
- For any data sharing requirement, it must be assessed if there is a legal obligation to share data (for example a statutory requirement, a court order, or any such similar obligation).

6.2. Agencies will:

- Share data with each other where it is lawful.
- Integrate and share data over the Oman Government Network.
- Ensure that information sharing is facilitated only over ITA Integration Broker and no direct point-to-point integration is established. (refer to the OeGAF Information Reference Model and the OeGAF Application Reference Model for standards related to information sharing)
- Publish the core data that belong to the Agency by developing Data Exchange Web services.
- Develop the “Process Web service” in order to facilitate inter Ministry process to achieve the “whole of Government” service delivery approach.
- Comply with the requirements of legal frameworks that govern data protection.
- Inform users when and how data is recorded about them and how their data may be used.
- Adopt as much as possible the 'once-only' principle. Once one principle is to ensure that entity will not ask citizens and businesses for the same information twice, and where upon login the entity will not ask for information that are available with the Government systems. Such Information should be integrated and collected from respective Government systems and not asked from the citizens or Business to be provided again. For example the commercial Registration number with Invest Easy System or Person ID from the National Registration System.
- Ensure that adequate technical and non-technical security measures are applied to the personal data being held and transferred.

- When sharing data to external non-government entity, the sharing agency needs to acquire special security clearance by from ITA's Information Security division.
- Promote staff awareness of the information sharing policies and procedures.
- Promote awareness of the need for information sharing through appropriate media.

7. Organisational and Individual Responsibilities

7.1. Agencies are responsible for embedding this policy within their own organization policies relating to information sharing, if any.

7.2. All agencies should appoint an authority for ensuring all information sharing responsibilities of the agency. This may comprise of person(s) who are from departments such as Risk Management or Information Technology and who have sufficient understanding of the policies and procedures for information sharing.

7.3. Information received by agencies as part of an information sharing arrangement, shall not be further released to any third party or to another agency without the permission of the owner agency.

7.4. Agencies need to adhere to a number of safeguards in order to ensure a balance between maintaining confidentiality and sharing data appropriately. These are:

7.4.1. Ensure staff are aware of and comply with:

- Their responsibilities and obligations with regard to the confidentiality of personal data about people who are in contact with their agency.
- Know whom to contact, and processes to follow, in the event of a breach of confidentiality.
- the commitment of the agency to share data legally and within the terms of an agreed specific information sharing arrangement
- the commitment that data will only be shared on a need-to-know basis
- their responsibilities and obligations with regard to sharing data with a Third Party

7.4.2. Ensure information disclosed is recorded appropriately by:

- Putting in place procedures to record the details of the information shared, the provider and who received the information.

7.4.3. Ensure that individuals are aware of whom to contact if queries arise.

7.4.4. **Data security**

Agencies shall ensure appropriate measures are in place to protect the confidentiality, integrity and availability of the data during all stages of processing. Agencies need to comply with the Information Security procedures and policies as published by ITA.

7.4.5. **Data quality**

Data shared should be of a good quality and it is recommended that the data shared follows appropriate guidance used by the agency sharing the data. As a general guidance, the following six data quality principles may be applied:

- Accuracy – Data should be sufficiently accurate for their intended purposes, represented clearly and in enough details. Data should be captured once only, although they may have multiple uses.
- Validity – Data should be recorded and used in compliance with relevant requirements, including the correct application of any rules or definitions. This will ensure consistency of the data when compared during the same time periods between different organizations.
- Reliability – Data should reflect stable and consistent data collection processes across collection points and over a period of time, whether using manual or computer based systems, or a combination.
- Timeliness – Data should be captured as quickly as possible after the event or activity and must be available for the intended use within a reasonable time period. Data must be available quickly and frequently enough to support information needs and to influence service or management decisions.
- Relevance – Data captured should be relevant to the purposes for which they are used. This entails periodic review of requirements to reflect changing needs.
- Completeness – Data requirements should be clearly specified based on the information needs of the agency and data collection processes matched to these requirements. Monitoring missing, incomplete, or invalid records can provide an indication of data quality and can also point to problems in the recording of certain data items.

8. Monitoring and review

8.1. ITA, in conjunction with appropriate representation from agencies, shall review this policy on a yearly basis unless new or revised legislation necessitates an earlier review.

8.2. Each agency will be responsible for periodically monitoring and reviewing the implementation of the policy and procedures in their organisation.

8.3. Each agency will be responsible for periodically monitoring and reviewing the personal information sharing arrangements they may have.

9. Breaches

9.1. Agencies will have in place appropriate measures to investigate and deal with the inappropriate or unauthorised access to, or use of, personal data whether intentional or unintentional.

9.2. In the event that personal data shared in accordance with this policy and supporting procedures is or may have been compromised, whether accidental or intentional, the agency making the discovery will, without delay:

- take appropriate steps, where possible, to mitigate any impacts
- inform the agency which provided the data of the details
- take steps to investigate the cause
- take disciplinary action against the person(s) responsible, whenever appropriate.
- take appropriate steps to avoid repetition of similar conduct.

9.3. On being notified of a breach, the original data provider, along with the agency responsible for the breach, and others, as appropriate, will assess the potential implications.

9.4. Where a breach is identified as serious, it shall be reported to the Integration and Shared Services Department of ITA. The original data provider, along with the breaching organisation and others, as appropriate, will assess the potential implications, identify and agree on appropriate actions.

10. Complaints

10.1. Agencies must have procedures in place to address complaints relating to the disclosure of personal data. The agencies shall agree to cooperate in any complaint investigation where they have data that is relevant to the investigation. Agencies must also ensure that their complaints procedures are well publicised.

10.2. If the complaint affects more than one agency, it should be brought to the attention of the respective authorities (responsible for information sharing) which should then liaise to investigate the complaint.

SIGNED ON

Signed for and on behalf of))
Information Technology Authority by:))
))
))
))

_____

H.E. Dr. Ahmed Mohammed Salem Al-Futaisi

Chairman of Board

Information Technology Authority