وزارة الاتصالات وتكنولوجيا المعلومات
Ministry of Information and Communications Technology

Data Management Policy

Ministry of Information & Communications Technology (ictQATAR)

May 2015

Table of Contents

Definitions and Acronyms

"**Agency**" means Government Agency, unless the term is used or referred to in a specifically different context

"The **British Computer Society or** the **BCS**" is an international professional body and a learned society with the objectives to promote the study and application of communications technology and computing technology and to advance knowledge of education in ICT for the benefit of professional practitioners and the general public. The BCS is the only professional body in the United Kingdom with the ability to grant chartered status to IT professionals under its Royal Charter, granted to them by the Privy Council

"**DAMA** (the **Data Management Association**)" is a not-for-profit, vendor-independent, international association of technical and business professionals dedicated to advancing the concepts and practices of information resource management (IRM) and data resource management (DRM).

"**Data**" and its management for the purpose of this document refers to all data and information in electronic form that Government Agencies capture, retrieve, share or process for the provision of e-Services to public, visitors and businesses.

"**Data Processing**" for the purpose of this document means the carrying out of any operation or set of operations on data, including the collection, receipt, recording, organizing, storing, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, transmission, blocking, erasure, or destruction of such information

"**Data Sharing**" means the disclosure of data form one or more agency/entity to a third party Agency/entity or Agencies/entities, or the sharing of data between parts of an Agency/entity

"**Data Source Agency**" means the Agency where the data is recorded, maintained and established as the rightful source for the given dataset(s), and that provides/shares the data with other agencies

"**Data User Agency**" means the Agency that requests/receives the data

"**Electronic Data**" means all data in electronic format, structured or unstructured

"**Government Agency**" refers to all ministries and public institutions directly reporting to Ministries or Council of Ministers in the State of Qatar

"**ictQATAR**" refers to the Ministry of Information and Communications Technology of the State of Qatar, previously known as the Supreme Council of Information & Communication Technology

"**Personal Data**" refers to (i) any information about an individual whose identity is apparent or can reasonably be ascertained either from that information or from a combination of that and other information; and/or (ii) any information, including location data, that can reasonably be linked to a specific individual irrespective of whether or not the identity of the individual is apparent from that information or from a combination of that and other information

"**Third Party**" for the purpose of this document shall mean any person or entity, other than the Data Source and Data User Agencies, that carries out data processing on behalf of an Agency and shall include any other person or entity appointed by a Third Party for the said purpose.

1 *Legal Mandate*

Article 14 of Emiri Decision No. 16 of 2014 setting the mandate of Ministry of Information and Communications Technology (hereinafter referred to as "ictQATAR") provides that ictQATAR has the authority to supervise, regulate and develop the sectors of Information and Communications Technology (hereinafter "ICT") in the State of Qatar in a manner consistent with the requirements of national development goals, with the objectives to create an environment suitable for fair competition, support the development and stimulate investment in these sectors; to secure and raise efficiency of information and technological infrastructure; to implement and supervise e-government programs; and to promote community awareness of the importance of ICT to improve individual's life and community and build knowledge-based society and digital economy.

Article 12 (9) of Emiri Decision No. 27 of 2014 setting the organization structure of the ictQATAR provides it with the authority to draft legislations, policies and standards for information technology systems, electronic transactions and e-government services to enable the transformation of government agencies in the State of Qatar.

The Government has set out the vision to ensure that information will be shared to provide better public services through greater cross-agency coordination. The National Development Strategy 2011-2016 has identified the use of ICT to achieve "institutional integration" through greater integration of processes, establishing central data repositories to deliver citizen-centric public services. Greater coordination through sharing of information will reduce fragmentation in decision-making by the government agencies.

This Policy Document has been prepared taking into consideration current applicable laws of the State of Qatar. In the event that a conflict arises between this document and the laws of Qatar, the latter, shall take precedence. Any such term shall, to that extent be omitted from this Policy Document, and the rest of the document shall stand without affecting the remaining provisions. Amendments in that case shall then be required to ensure compliance with the relevant applicable laws of the State of Qatar.

2 Introduction

The primary objective of data management is to support the business information needs of an organization[1]. Data management may be defined[2] as the practices, architectural techniques and tools for achieving consistent access to and delivery of data across the spectrum of data subject areas and data structure types in the enterprise, to meet the data consumption requirements of all applications and business processes. From a service perspective, data management is viewed[3] as a corporate service which helps with the provision of information services by controlling or coordinating the definitions or usage of reliable and relevant data. Key Data Management activities[4] include:

- Data Policy development;
- Data Ownership;
- Metadata Compilation;
- Data Lifecycle Control;
- Data Quality; and
- Data Access and Dissemination.

This document takes into account both management and service functions of data management processes while defining policy provisions, to support the business information need for delivering seamless government services to the public.

2.1 Background

As we move into a knowledge-based economy, information becomes a valuable asset that the Government must manage as a public trust on behalf of its people. The effective use of data within and across public agencies is critical to enhance the ability of the government agencies to formulate policies and to deliver more convenient and citizen-centric services to the public.

The Government Agencies depend on information that may be owned by multiple agencies, to deliver public services to its people. They collect, use and store a wide range of personal information, such as date of birth records, national ID information, demographic and contact

[1] *Why Data Management*, DAMA International Foundation
[2] *Definition of Data Management and Integration, IT Glossary*, Gartner
[3] *Principles of Data Management, Facilitating Information Sharing*, the British Computer Society
[4] *The Principles of Good Data Management*, Office of the Deputy Prime Minister: London

details, in order to carry out their work. Information is used to check identity, confirm eligibility and to detect and prevent fraud.

It is, therefore, important that data is managed as a national asset. Managing information as an asset will increase operational efficiencies, reduce costs, improve services and promote better governance. This policy document aims at establishing governance and standard processes across the Government Agencies in the State of Qatar for managing and sharing data.

2.2 Current Situation

Some Government Agencies are currently exchanging information to enable the efficient delivery of services to the public. For example, Ministry of Interior, Supreme Council of Health, Ministry of Labor and Social Affairs, Ministry of Economy and Commerce and Ministry of Development Planning and Statistics have established direct arrangements for such data exchanges via various electronic and non-electronic means. However, such data exchanges are currently conducted on a limited one-to-one basis.

There are agencies that may not know that data exists in the public sector. Even if they know the data exists, they may not know where it resides or how to procure it. At times, there can be situations where data may be acquired from another agency, but they cannot let their customers know that they exist (i.e. prohibited by agency supplying the data). Some agencies may also be apprehensive of releasing/sharing data under the impression that any such information sharing may be construed as inappropriate disclosure of data and possibly an offence.

Even if the agencies are willing to share data with each other, data may not be available in electronic form; appropriate data management processes may not be in place such as data protection and data standards; or an appropriate channel or platform may not be available for electronic sharing of data. Similarly, some government agencies may decide not to pursue new data sharing initiatives because of doubts over what their legal powers allow them to do. These problems are more pronounced when data need to be procured from multiple agencies for delivery of a service.

At the same time, in a survey[5], internet users in the GCC have voiced concerns about repurposing of personal data that they have provided for one purpose.

[5] ictQATAR's report in July 2014 on *The attitudes of online users in the MENA region to Cybersafety, Security and Data Privacy* (Page 29: Concerns around the repurposing of personal data)

2.3 The Need for Data Management and Sharing

At the heart of the problem of information management and sharing is that most of the data within government is contained in "silos", in other words within separate departments. While the data may be effectively managed at individual agencies, a standard approach to managing data will lead to greater level of interoperability and thus more effective government-wide data sharing.

Governments across the globe have recognized the importance of data management and sharing, and have established legislations, practices and processes to facilitate the same. Executive Office of the President of the US[6] has directed the heads of executive departments and agencies to manage information as an asset and established a framework to help institutionalize the principles of effective information management at each stage of the information's life cycle to promote interoperability and openness. Canada's[7] Information Management policy advocates managing information and records using a whole-of-government approach. Finland[8] has introduced a law on information management governance that lays down provisions on the obligations of certain authorities in public administration when conducting information management tasks including availability of information in electronic form, system interoperability, and information exchange. The New Zealand[9] Parliament amended the privacy act allowing approved information sharing agreements to enable the use and sharing of information between and within agencies delivering public services by modifying or clarifying the application of the information privacy principles. Australia[10] has established a national strategy with the key aim of managing government information as a strategic asset providing more efficient and effective use of it. The Law Commission in the United Kingdom[11] set up for the purpose of promoting the reform of the law, has presented a report on data sharing between public bodies before the Parliament, recommending a full law reform in order to create a principled and clear legal structure for data sharing for efficient and effective government, the delivery of public services and the protection of privacy; as well as establishing codes of practice in the management of data sharing between public bodies.

In order for the State of Qatar to bring about more effective usage of data in the public sector within the ambit of current legislations and maintaining essential protection and privacy of the data, Ministry of Information and Communications Technology (ictQATAR) has taken the lead

[6] *Memorandum for the Heads of Executive Departments and Agencies: Open Data Policy-Managing Information as an Asset*, 9 May 2013; Office of Management and Budget, Executive Office of the President of the United States of America

[7] *Policy on Information Management*, 1 July 2007; Treasury Board of Canada Secretariat, Government of Canada

[8] *Act on Information Management Governance in Public Administration*, 1 September 2010; Ministry of Finance, Finland Government

[9] *Information sharing changes to the Privacy Act 1993*, February 2013; New Zealand Government

[10] *National Government Information Sharing Strategy*, July 2007; Australian Government Information Management Office; Commissioned by Council of Australian Government's Online and Communication Council, Australian Government

[11] *Data Sharing between Public Bodies, A Scoping Report*, 10 July 2014; The Law Commission, Ministry of Justice, United Kingdom

to develop a Policy that will guide agencies in data management and sharing across the public sector. This policy document seeks to empower and guide the Government Agencies in Qatar to manage and share data within the prevailing laws in order to facilitate efficient delivery of government services while ensuring information and privacy protection.

As a further step, ictQATAR also plans to develop an application platform to facilitate cross agency data exchange.

2.4 Guiding Principles

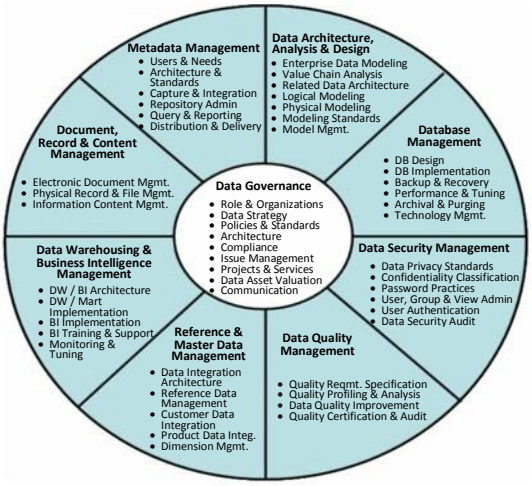
The policy aim of this document is to provide a basis that any data that will be shared is used only for legitimate purposes, and to lay the foundation for effective data management. Where government collects, holds or uses personal information, it must act as the custodian of that data and retain and protect the information securely in accordance to the provisions of the relevant laws, legislations and policies. It defines the rules for agencies to facilitate effective intra and inter-agency data sharing.

The following are the key guiding principles applied in drafting this policy:

i. Data should be managed as a strategic resource that supports policy and decision-making, accountability and the efficient delivery of government programs and services;

ii. Data collected or generated by each agency should not be viewed as belonging to one agency alone but is available for sharing with other agencies, within the bounds of privacy, copyright, legal and security considerations;

iii. Where possible, capture data once and use it for multiple and/or generic purposes, avoiding duplication in data acquisition.



The DAMA DMBOK[12] Framework identifies the ten functions of data management as shown in the adjacent figure. This document draws from this framework relevant functions for policy purposes.

[12] Data Management Body of Knowledge, A publication by the Data Management Association or DAMA (www.dama.org)

3 Scope and Application

3.1 This policy governs how data is managed and exchanged in Government Agencies.

3.2 This Data Management Policy comprises the following core domain areas:

i Data Governance;

ii Data Administration;

iii Data Protection; and

iv Data Sharing.

3.3 This policy applies to all electronic (structured or unstructured) Data that is created, collected and maintained by Agencies as part of their official business functions and used or shared for the purpose of provision of public services. Examples of structured data include customer data (such as personal data and corporate data), non-customer data (such as environment data) and organizational data (such as HR, finance, asset and procurement-related data). Unstructured data (such as word processor documents, presentation slides, pictures, videos and audios) include both text-based and bitmap-based data.

3.4 This policy on Data Management operates subject to privacy, copyright, legal and security considerations. Agencies should ensure that they are compliant to the relevant legislations[13] applicable in the State of Qatar.

[13] Legislations include decrees, directives, laws and policies issued by relevant authorities in Qatar

4 Policy Provisions

This section provides provisions for Government Agencies in the State of Qatar to ensure that data are properly managed, protected and also exchanged between them for delivery of efficient services to the public.

This policy on Data Management requires all Government Agencies in the State of Qatar to take the following steps:

4.1 Data Governance

i. Agencies shall assign a senior official, whose responsibility is to oversee the management and control of the Agency's data and related processes.

ii. The role of the senior official should be assumed by an officer of sufficient seniority as the officer shall have to oversee and represent the agency in all data management and cross-agency data sharing matters and issues.

iii. The appointed official shall ensure that proper information lifecycle management[14] processes and procedures are in place to create, store, manage and process data that is accurate, timely and complete. He/she shall also be responsible for ensuring compliance with relevant legislations in this respect.

iv. All inter-agency issues related to cross-agency data management and sharing shall be escalated to the e-Government Steering Committee. The e-Government Steering Committee will oversee, ensure alignment and provide overall guidance and advice on data management issues to facilitate data sharing across agencies within the current legislative framework.

4.2 Data Administration

4.2.1 Data Ownership

i. Data collected by any Agency eventually belongs to the Government of Qatar and as such should be available for sharing with other agencies, within the constraints of existing laws, policies and regulations.

[14] Please refer to Appendix 1 for guidelines

ii. Data Source Agencies shall put in place data maintenance processes including handling any subsequent data updates and disseminations to the Data User Agencies.

iii. To ensure integrity of data across government, Agencies shall first source data required to complete service transaction from Data Source Agencies, if available. If there is no Data Source Agency for the required data, then the Agencies may collect data from other valid sources.

4.2.2 Data Collection

i. Agencies shall ensure that all information or records are stored electronically in their systems, classified and secured in line with the National Information Assurance Policy v2.0. Agencies shall also establish and maintain a register of such key data and information assets.

ii. Agencies shall ensure that data is collected by lawful and fair means, and is limited to that which is necessary to fulfil its statutory or business requirements. Policy provision 4.2.1 (iii) in this document shall be applied in determining whether the Agency should source data from another Agency (Data Source Agency) or collect from other valid sources.

iii. Agencies should request for supportive information or documents from individuals or businesses to process service transactions only when such information is not available electronically with them or not available for sharing electronically by any other government agency.

iv. Agencies shall ensure that the individual to whom the Personal Data relates, has knowledge of and has given consent for the collection, use or disclosure of Personal Data to a Third Party or another Agency for the purpose of service transactions processing.

v. Agencies shall conduct reviews to identify services where document submissions and form filling by individuals and businesses can be eliminated or reduced to a minimum:

(a) conduct reviews to determine if the information or document is needed to process the particular service or transaction;

(b) consider alternative means of information sourcing through:

- sourcing needed information internally from repositories and databases;
- seeking the needed verifications and/or required data externally from the Data Source Agencies;
- automating the above process of internal or external information sourcing;

4.2.3 Data Standards

Data standards are the foundation for interoperability. The adoption of a set of data standards for use across the government agencies will remove ambiguities and inconsistencies in the use of data and enable more effective use and exchange of data.

i. Each Agency shall be responsible to establish and maintain data standards catalogue[15] that shall include metadata information and standards for their data in a standard format. Data standard catalogue shall also help establish a primary business owner or Data Source Agency for a particular data.

ii. Agencies shall disseminate data standards catalogue to authorized personnel at other Government Agencies to determine availability of data as well as metadata information and standards.

iii. Data User Agencies shall adopt data standards of the Data Source Agencies for the given data elements.

iv. Data Source Agency shall be responsible for updating their data standards catalogue with new or updated attributes and notify statewide stakeholders for all revisions.

4.2.4 Data Access

Data access is granted only to individuals and agencies that have legitimate and justifiable reasons for access, within the bounds of relevant laws, policies and regulations.

[15] Please refer Appendix 2 for data standards template and example

i. Agencies shall clearly distinguish between data items for controlled access from items for open access that are classified as *public* in line with the National Information Assurance Policy v2.0.

ii. Agencies shall put in place controls to ensure that access to controlled data is granted only to individuals, entities or other Agencies that have legitimate and justifiable reasons for such access, as well as appropriate approval clearance.

4.3 Data Protection

4.3.1 Protection of Information and Data

Each agency is responsible for protection of all data, including personal data in its custody.

i. Agencies shall protect all information and data in their possession (including data received from other Agencies), or when disclosing data to a Third Party or another Agency. Security safeguards shall be put in place to protect data against any unauthorized access, and disclosure or modification.

ii. Agencies shall adhere to ictQATAR's National Information Assurance Policy v2.0 to ensure adequate safeguards are in place to protect any systems and electronic storage media that handle data to prevent any unauthorized access, or modification to the data.

iii. Agencies shall conduct periodic review of their policies and processes to ensure adequate data safeguard, and conduct periodic audits to ensure that the measures to safeguard data are in compliance with the policies.

iv. Agencies shall ensure processes are in place to protect confidentiality and integrity of data obtained from other agencies.

v. Agencies shall ensure that all data and information assets are classified and stored according to their security level (please refer to ictQATAR's National Information Assurance Policy v2.0).

4.3.2 Protection of Personal Data

i. Agencies shall adhere to information privacy principles and applicable laws in the State of Qatar for the collection, processing and sharing of Personal Data.

Agencies shall also ensure its policies and processes for the protection of Personal Data are up-to-date and are strictly adhered to for all data processing within the Agency and when transferring or sharing data with another Agency or to a Third Party.

ii. Agencies shall ensure that their policies and processes with respect to the processing of Personal Data cover:

(a) Personal Data held by the Agency or which is made available to other Agencies are necessary for the purposes of fulfilling a legal or regulatory requirement, or for delivering a public service;

(b) procedures for an individual to obtain more information on or gain access to the Personal Data which the individual has earlier provided to the Agency, and on the use and disclosure of such Personal Data by the Agency; and

(c) contact details of the officer-in-charge, to whom enquiries or feedback on Personal Data can be forwarded.

iii. Agencies shall publish a Privacy Statement on their website. Please refer to Appendix 3 for sample copy of Privacy Statement.

iv. Agencies shall implement processes to dispose of or destroy Personal Data securely so as to prevent unauthorized parties from gaining access to these data.

4.4 Data Sharing and Usage

4.4.1 Sharing of Data

Agencies should not be collecting data from the public if the data is available from other government agencies. This will ensure that the public would only need to supply data only once to the government agencies in order to obtain various services; thereby ensuring single source of truth, and data accuracy and integrity.

i. Data Source Agencies shall share the data captured or generated with other Agencies in compliance with legal and privacy obligations, so long as there is a clear and valid purpose for sharing.

ii. Agencies shall obtain consent from individuals in the hard-copy or online service application form, allowing re-use and sharing of personal data for the purpose of

provision of government services to them. Such consent may be in the form of a statement that by applying for the requested service, the applicant henceforth allows for sharing and re-use of his or her personal data between Government Agencies in the State of Qatar, solely for the purpose of provision of current and future requested government services to them.

iii. For re-using or sharing such data for any purpose other than provision of services, Agencies shall seek individual's consent for such specific purposes.

iv. Data Source agencies shall facilitate and enable the sharing of data with data user agencies so that the public sector can:

(a) bring greater convenience to individuals and entities (such that they need only to supply data once to the Government of Qatar in order to obtain various public services, instead of having to supply same data to different Agencies for various transactions);

(b) enable the delivery of end-to-end e-Services (as provided for under ictQATAR's national eGov2020 strategy);

(c) develop more informed and targeted policies through access to more and better quality data; and

(d) enhance efficiency and reduce cost through increased data sharing.

4.4.2 Purpose of Data Sharing

Agencies shall share data with one another only for clear and valid purposes.

i. Data User Agencies shall establish a clear purpose to the Data Source Agency, unless the Data has been pre-approved for use for all purposes by the Data Source Agency.

ii. Data User Agencies shall use data for its specified purposes only.

iii. Where appropriate, data sharing agreements should be established to bind all parties involved in the sharing initiative. Such a data sharing agreement should include: purpose of data sharing, organizations involved, datasets/ items to be shared, rules for retention and deletion of shared data items, procedures for dealing with termination of data sharing agreement.

4.4.3 Sharing within the Government

i. Data collected or generated by an Agency shall be shared with other Agencies, within the bounds permissible by applicable laws and the principles of data privacy , to allow the government agencies to achieve the objectives of:

(a) delivering customer-centric services;

(b) achieving quality policy formulation;

(c) facilitating analysis and research.

ii. For sensitive data, the Data Source Agencies shall work with the Data User Agencies to determine the minimum amount of data necessary to meet the user needs while ensuring adequate safeguards are in place to protect the data; for example, by determining if the objective can be achieved by anonymizing them.

iii. Data to be shared should be limited to what may be necessary for the purposes of the request. For example, if the purpose of the data request is to verify if the applicant earns less than QAR 10,000 to qualify for certain social benefits, the data users should ask for income indicators i.e. “Yes” if income is more than QAR 10,000 or “No” if income is less than QAR 10,000, instead of the absolute figure for the income of the individual.

iv. Where possible, Data User Agencies shall comply with the data standards of Data Source Agencies to ensure easy availability of data.

v. Where the data standards of the Data Source Agencies are rendered not suitable for exchange or delivery of services by the Data User Agencies based on legitimate and justifiable reasons, the former shall update the existing data standards and make the data available in the agreed format within reasonable timeframe.

vi. Agencies engaged in data sharing shall put in place processes to handle data updates and feedback on the data quality.

vii. Agencies shall clearly stipulate the conditions for using, handling and disposing of the data before the data is transferred to the Data User Agencies, including retention periods and deletion arrangements for the data sent or received.

viii. Data User Agencies shall not share data with other Agencies without the explicit approval of the Data Source Agency, unless otherwise authorized or required by law or decree, or the data is pre-approved for use for all purposes by the Data Source Agency.

ix. Data Source Agencies shall share all data as "pre-approved for use for all purposes" through the Central IT Platform (refer 4.5 below) for data exchange services for re-use by Government Agencies.

4.4.4 Sharing with General Public

i. Agencies shall share only non-Personal Data with the general public within the ambit of relevant laws, policies and regulations.

If the data is not owned by the Agency, it shall seek approval from the Data Source Agency before releasing such data to the general public unless otherwise authorized or required by law or decree.

4.5 Central IT Platform to Support Government Data Exchange

i. ictQATAR shall establish and maintain a Government Data Exchange Platform that would allow agencies to share and access available data to deliver public services, and would comprise the following core components:

(a) IT infrastructure – a secure government data exchange IT platform that would allow Data Source Agencies to share data while Data User Agencies will be able to search and request for available data ;

(b) Data Standards Catalogue – compiled and updated available data dictionaries of all Government Agencies as defined in section 4.2.3 (i), that shall include metadata information and standards

(c) Platform Management & Governance – establish the governing structure and processes to oversee the effective and efficient use of data among government agencies including Terms Governing Use and Access, SLAs, etc.

ii. All Agencies shall share and exchange data with other government agencies in the State of Qatar through the Government Data Exchange Platform as and when it becomes operational, and adhere to the governing processes and standards.

4.6 Implementation Progress & Review

ictQATAR as the Policy owner of the Data Management Policy will monitor agencies' implementation and compliance to this Policy and access to the central IT Data Exchange Platform, as and when it is developed.

i. Agencies shall undertake its utmost efforts to share data between the government agencies so as to deliver end-to-end e-Government services to better serve the people of Qatar.

ii. Ministry of Information and Communication Technology (ictQATAR) may issue any additional or supplementary procedures, guidelines and best practices from time to time to support the Data Management Policy.

APPENDICES

Appendix 1: Information Lifecycle Management

Appendix 2: Data Standards Template

Appendix 3: Sample of a Privacy Statement

Appendix 1: Information Lifecycle Management

This section presents a concise guide for understanding various steps involved in the information lifecycle management process for Agencies to establish relevant operational policies and procedures for effective data management.

Information Lifecycle Management (ILM) is an approach to management of enterprise records, data and information (hereinafter referred to as "data" within this section for ease of reference) through their lifecycle, i.e. from their inception until disposal. It is based on the premise that the value of data changes over time and that it must be managed accordingly.

ILM covers three key stages – (i) create and capture, (ii) store and manage, and (iii) distribute and transact:

i. Create and Capture

The first stage involves creating or capturing data in a digital form. Some data may be *born* digital, for example output such as an xml file from a system or data available in digital format such as spreadsheet received from other sources. While non-digital data from other sources such as paper documents may be digitized through manual input into a system or scanning solutions.

The process for capturing and storing digitally sourced data is relatively easier as compared to creating digital data from non-digital sources. Technical solutions to assist in the process of creating and capturing data include digital forms, document management solutions, scanning and image capturing solutions, and system integration solutions.

Agencies should put in place processes and procedures that are in compliance with Qatar's Law Number 2 of 2011 on Official Statistics where required, to cover all aspects of creating and capturing data, and as far as possible automate the process steps.

ii. Store and Manage

Once the data is collected and created, it must be stored in a manner that best supports business processes. The second stage involves managing the data captured and stored in the organization's IT infrastructure as per its operational policies. Key elements at this stage of ILM include:

a. *Data classification*

The rationale for classifying information into classes is to allow appropriate values to be ascertained for information items, their risks to be determined, and the corresponding protection to be applied. All data created and captured must be classified in accordance with the National Information Assurance Policy v2.0.

b. *Data security and accessibility*

Physical security, network security and security of computer systems and files all need to be considered to ensure security of data and prevent unauthorized access, changes to data, disclosure or destruction of data. Security arrangements need to be proportionate to the nature of the data and the risks involved.

Other important steps in this process to aid in discovery and accessibility are indexing the data and exposing discovery metadata through searchable interface.

Listed below are certain data security practices:

- Physical data security requires:
  - controlling access to rooms and buildings where data, computers or media are held
  - logging the removal of, and access to, media or hardcopy material in store rooms
  - transporting sensitive data only under exceptional circumstances, even for repair purposes, e.g. giving a failed hard drive containing sensitive data to a computer manufacturer may cause a breach of security

- Network security means:
  - not storing confidential data such as those containing personal information on servers or computers connected to an external network, particularly servers that host internet services
  - firewall protection and security-related upgrades and patches to operating systems to avoid viruses and malicious code

- Security of computer systems and files may include:
  - locking computer systems with a password and installing a firewall system
  - protecting servers by power surge protection systems through line-interactive uninterruptible power supply (UPS) systems
  - implementing password protection of, and controlled access to, data files, e.g. no access, read only, read and write or administrator-only permission
  - controlling access to restricted materials with encryption
  - imposing non-disclosure agreements for managers or users of confidential data
  - not sending personal or confidential data via email or other file transfer means without first encrypting them
  - destroying data in a consistent manner when needed
  - not using file sharing services such as Google Docs or Dropbox that may not be secure
  - enabling audit trail and version control to track modifications to systems and databases

- Security of personal data:

  Data that contain personal information should be treated with higher levels of security than data which do not. Security can be made easier by:
  - anonymizing or aggregating data
  - removing personal information, such as names and addresses, from data files and storing them separately
  - encrypting data containing personal information before they are stored - encryption should certainly be needed before transmission of such data.

Agencies should define information security processes and procedures in line with National Information Assurance Policy v2.0.

c. Data quality

Data is considered to be of good quality if it is complete, accurate, available and timely. Common errors affecting data quality include duplicate master records, lack of common standards and absence of links between transactional elements.

Key steps of the data quality process are:

- Data assessment:

  Data assessment phase consists of analyzing the data structures and end to end mapping between source and destination systems. This stage defines the data cleansing requirements and sets priorities.

- Data quality control:

  This phase focusses on correcting and standardizing the data to control the data integrity over time, and mainly involves three steps: data standardization, data cleansing and data consolidation. While data standardization ensures consistency of data across systems, data cleansing is carried out to ensure integrity of data and to prepare the data for specific migration needs. Data consolidation reduces duplicate and unnecessary information in data repository.

- Data quality verification:

  Cyclic tests should be conducted to check for any data errors. Data validation gives visibility into the errors, their causes and possible remedial actions.

Agencies should establish a continuous and iterative data quality framework to control data quality.

d. Data Backup

The primary purpose of backup is to recover data after its loss, be it by data deletion or corruption. Backup is generally part of organizational disaster recovery plans. Agencies should put in place backup processes in alignment with the National Information Assurance Policy v2.0 and their disaster recovery policies and procedures.

e. Data disposal and archival

Data disposal means securely erasing the data that has become obsolete or redundant and is not required to be maintained or preserved; while archival refers to the process of identifying and moving inactive data out of current production systems and into specialized long-term archival storage systems.

One key step in this process would be to define organizational data retention policies. Below are certain legal and regulatory provisions applicable in Qatar[16] pertaining to record retention:

- Records relating to *customer identification* must be maintained for 6 years from the *end* of the relationship (QFC Anti-money laundering Regulations, art. 10).
- The *account books of all Traders (including companies) and Foundations* must be maintained for 10 years, and the *underlying documentation* must be maintained for 5 years (Commercial Law, art. 28).
- *Taxpayers* carrying on an activity in Qatar are required to keep *accounting books, registers and documents* in accordance with international accounting standards (Income Tax Law, art. 18) and these must be maintained for 10 years in the place where the activity is carried on (Income Tax Law, art. 19).
- *All QFC entities* must maintain *accounting records* until the later of 6 years from the end of the accounting period or the completion of any enquiries into the return for the accounting period (*LLC:* QFC Companies Regulations, art. 79; *LP:* QFC Partnership Regulations, art. 62; *LLP:* QFC Limited Liability Partnership Regulations, art. 34; *Branches of non-QFC partnerships registered in the QFC:* QFC Partnership Regulations, art. 81):

Agencies should review all applicable legislations, regulations and standards, and define data retention policies based on the scope of application over types of data generated and maintained by them, in alignment with National Information Assurance Policy v2.0 (Section 11 - Data Retention & Archival, Part B - Security Governance & Security Processes, National Information Assurance Manual). Agencies

[16] Above cited examples of the laws are for reference only and do not necessarily form an exhaustive list; Agencies should review all applicable legislations for defining data retention policies. Legislations, policies etc. are subject to amendments and changes, and should be periodically reviewed in order to ensure currency and applicability due to amendments or changes.

should also establish secure data disposal and archival processes based on the policies defined.

iii. Distribute and Transact

During this stage, data once captured and stored is often sent to a workflow for routing and action as part of business process. To process the data, it is actively being accessed and shared by government agencies and their employees in this stage. The rules for who can access each record will have been determined in the previous stage, providing the right environment for easy access to timely, accurate and available information within security and privacy guidelines. Agencies should establish processes for easy discovery and access of input data, and management of output data.

Appendix 2: Data Standards Template

Reference Number	Data Element	Description	Format	Length	Value (Example)	XML Tag	XML Schema	Parent Data Element	Child Data Elements	Custodian Agency	Custodian Department	System of Record	Latest Version	Date Published (dd/mm/yyyy)	Comments
Example*															
1.0.0	Address Structure	Represents address structure in Qatar				AddressStructure	Address-v2-0.xsd	[Root element]	BuildingNumber LocalityInformation CityInformation	Agency X	Department Y	System Z	2.0	16/01/2014	
1.1.0	Building Number	Identifies building number	Apha-numeric, Character	5	18-A	BuildingNumber	Building-v1-0.xsd	AddressStructure		Agency X	Department Y	System Z	1.0	01/09/2013	
1.2.0	Locality Information	Identifies locality in a City				LocalityInformation	Locality-v1-1.xsd	AddressStructure	LocalityName StreetName ZoneNumber	Agency X	Department Y	System Z	1.1	16/01/2014	
1.2.1	Locality Name	Identifies locality name	Alpha-numeric, Character	30	Al-Markhiya	LocalityName	LocalName-v1-0.xsd	LocalityInformation		Agency X	Department Y	System Z	1.0	01/09/2013	
1.2.2	Street Name	Identifies street information	Alpha-numeric, Character	30	Al-Khalifa	StreetName	Street-v1-0.xsd	LocalityInformation		Agency X	Department Y	System Z	1.0	01/09/2013	
1.2.3	Zone Number	Identifies zone code	Numeric	5	67	ZoneNumber	Zone-v1-1.xsd	LocalityInformation		Agency X	Department Y	System Z	1.1	16/01/2014	
1.3.0	City Name	Identifies city name	Alphabetic, Character	30	Doha	CityName	City-v1-0.xsd	AddressStructure		Agency X	Department Y	System Z	1.0	01/09/2013	
2.0.0	---	---	---	---	---	---	---	---	---	---	---	---	---	---	

* This is only an example and not a presentation of actual data standards

This template may evolve as more enterprise data standards are developed and Agencies continue to collaborate and coordinate.

Appendix 3: Sample of a Privacy Statement

This is a [Name of Ministry/Agency] website.

We are committed to protecting your privacy and providing a secure website environment. We take precautions to protect your information. When you submit sensitive information via the website, your information is protected both online and offline.

Information Collection, Use, Sharing and Rectification

If you are only browsing this website, we do not capture any information that allows us to identify you individually.

If you are making an online e-service application that contains your personal information, we may share such data with other Government agencies, or with non-Government entities which have been authorized to carry out specific Government services, so as to serve you in an efficient and effective way, unless such sharing is prohibited by law.

For your convenience, we may also display to you data you had previously provided us or other Government agencies. This will help speed up the transaction and save you the time of providing us the same information as in your past submissions.

Although we will undertake all reasonable efforts to keep your information updated, please do provide us with your latest information should you find the information not up-to-date.

Security

To safeguard your personal information, all electronic storage and transmission of personal data are secured with appropriate security technologies.

Links to External Websites

This site may contain links to external non-Government sites whose data protection and privacy practices may differ from ours. We are therefore not responsible for the content and privacy practices of these other websites.

Please contact us using our feedback form if:

(i) you have any enquiries or feedback on our data protection policies and procedures, or

(ii) you require more information on or access to the data which you have earlier provided to us.

Updates to Privacy Policy

Our Privacy Policy may change from time to time and all updates will be posted on this page.