Sultanate of Oman
Information Technology Authority

e.oman

Information Security Management Policy

Governance and Compliance Division

Document control:

Attributes	Value
Document title:	Information Security Policy
Document Owner:	Governance and Standards Division, ITA
Document Type:	Official
Document Approval:	CEO, ITA
Document Circulation:	All Ministries and Government Agencies

Revisions:

Version	Author	Date	Comments	Approved by
Draft 0.2	Governance and Standard Division, ITA	20 March 2018	Updated and revised contents	
Draft 0.3	Governance and Standard Division, ITA	3 Sep 2018	Updated and revised contents	
Final draft v1.0	Governance and Standard Division, ITA	20th Oct 2018	Internal reviews updated	
Final draft v1.1	Governance and Standard Division, ITA	6th Nov 2018	Internal reviews updated and revised contents	
Final draft v1.2	Governance and Standard Division, ITA	25th July 2019	ISD comments incorporated	
Final draft v1.3	Governance and Standard Division, ITA	25th July 2019	Internal reviews updated and revised contents	For approval by Management Committee

1 Contents

1. Introduction

Pursuant to, Royal Decree 52/2006, Information Technology Authority (ITA) is responsible for implementation of the Digital Oman Strategy and to provide professional leadership to government agencies. ‘Information’ has become a linchpin for success for any organization in any sector, hence to secure this vital ‘Information’, necessary precautionary measures need to be taken, so that an organization’s critical information is secure.

‘Information’ is data in the form of facts or ideas or knowledge in any form that can be communicated between system entities. Therefore, ‘Information Security’ is defined as “The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability”.

Henceforth, Information Technology Authority (ITA) is publishing ‘Information Security Policy’ for the whole of government, so that ‘Information’ can be handled in a better and secured way.

2. Purpose

The purpose of the Policy is to provide a consistent approach to managing information security across ALL Government Administrative Units and establish Information security management practices within the Government administrative units.

3. Scope

This Policy applies to ALL Government Administrative Units as custodians of information on behalf of the Sultanate of Oman.

4. Policy Principles

This Policy is based upon the following Information Security Policy principles:

- **Availability:** Information is accessible and usable to authorized entities.
- **Integrity:** The accuracy and completeness of information is protected.
- **Confidentiality:** Information is not made available or disclosed to unauthorized individuals, entities or processes.

Proportionality: measures to protect information are relative to the risk of loss or failure of availability, integrity and confidentiality.

5. Policy statements

5.1. Information Security Governance

Government agencies are required to establish an Information Security Committee composed of senior management or assign this role to an existing senior management committee. This steering committee shall be headed by ‘Undersecretary/Head of organization/CEO’ and have the representation from all senior management departmental/divisional heads i.e. Admin, finance, HR, senior business executives and IT directors.

The committee will be responsible to define the “Information security policy”*[1] for specific/individual agency*[2] and have following responsibilities:-

- Direct the development and maintenance of an agency’s ‘Information Security Program’
- Direct the implementation of Information Security Program
- Assign relevant responsibilities to the relevant staff:-
    - A dedicated role of ‘Information security officer’ shall be assigned
    - The ‘information security officer’ to report directly to the ‘Under-secretary’/CEO/Head of organization
- Control the maintenance and implementation of an agency’s communication plan for information security.
- The steering committee should ‘meet and review’ the effectiveness of information security program at least quarterly with ISO (Information Security Officer and his team).

5.2. Risk Management

Agencies shall conduct regular Information security *[3].risk assessments and implement appropriate “risk treatment” that are proportionate to the level of identified risk.

- Individual agencies are required to identify, quantify and prioritize risks against risk acceptance criteria, which should defined by steering committee and apply appropriate controls to protect against those risks.

**1. This 'information security policy' is required to be defined by each individual agency to satisfy information security requirements related to their specific business needs. As per already published ITA circular number: "3-2015 - General Information Security Policy"*
**2. "Individual agency "is referred to all "government administrative units", "government ministries" and "local government body/ authorities"*
**3. "IT Risk management framework" published by ITA can be referred*

5.3. Data classification

Agencies shall apply appropriate Data classification by:

- Applying information security classifications*[4.]
- Controlling physical access to information assets
- Controlling the use of information and communications technology

5.4. Training and Awareness

Agencies shall ensure that staff understand the Information security roles and responsibilities assigned to them:

- Appropriate level of training should be ensured for the 'information security officer'
- Implement and maintain an awareness and communication plan for relevant personnel.

5.5. Incident Management

Agencies shall ensure to have a structured approach to manage Information security incidents and events to support security program objectives:

- Agencies shall implement and maintain appropriate controls to mitigate the risks identified through incident management and risk assessment.

*4.
1. Royal Decree 118/2011 'Data Classification Law
2. 42/2015- Data Classification Law amendment
3. 26/2019- Data Classification Law amendment
4. "Data and Information Systems Security Classification Mapping" by Information Technology Authority (ITA)

5.6. IT Continuity Management

Agencies shall have a structured approach based on an Information security risk assessment, to manage IT Continuity to ensure uninterrupted availability of critical resources that support essential business activities.

- Each agency shall implement and maintain IT Continuity management controls that meet the requirements identified by risk assessment.

6. Roles and Responsibilities

6.1 Policy management

1. This policy is issued by Information Technology Authority (ITA).
2. Creation and maintenance of this IT Governance Policy is vested with the ITA.

6.2 Policy implementation

1. The Undersecretary/CEO of the government agency is responsible to ensure policy implementation and compliance according to the schedule given below.
2. ITA conduct policy compliance audits and report improvements in IT Governance and Management arrangements to the Cabinet of Ministers.

7. Implementation schedule

1. Assignment of Roles and Responsibilities through formal communication (first 3 months)
2. Define information security policy of individual agency (first 3 months)
3. Establishment of information security program (6 months)

Agency actions	Target date (From the date of publication of this Policy
1. Assign Roles and Responsibilities through formal communication.	3 months
2. Define Information Security Policy for individual agency *5	3 months
3. Establish the Information Security Program	6 months

**5.*
ITA circular number: 3-2015 'General Information Security Policy'
ITA circular number: 1-2017 'Security assessment of application & e-Services'

8. Related guidance

7.1. **Royal Decree 118/2011 'Data Classification Law**

7.2. **42/2015- Data Classification Law amendment**

7.3. **26/2019- Data Classification Law amendment**

7.4. **'IT Governance Policy'** by Information Technology Authority (ITA)

7.5. **IT Governance Charter** by Information Technology Authority (ITA)

7.5.1. **'Information Security Management Framework'** by Information Technology Authority (ITA)

7.6. **'IT Service Continuity Framework'** by Information Technology Authority (ITA)

7.7. **'IT Risk management framework'** by Information Technology Authority (ITA)

7.7.1. **"Data and Information Systems Security Classification Mapping"** by Information Technology Authority (ITA)

7.8. ITA circular number: **3-2015 'General Information Security Policy'**

7.9. ITA circular number: **1-2017 'Security assessment of application & e-Services'**