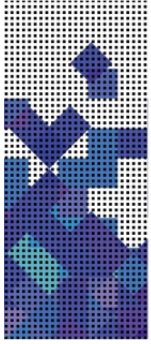

Sultanate of Oman
Information Technology Authority

Website and Data Hosting Policy

Governance & Standards Division

VALIDATION & DISTRIBUTION:

	Name	Email	Issue date
Issued by	Governance & Standards	standards@ita.gov.om	2017
Verified by			
Approved by	Steering Committee		

Distribution List	
1.	ITA
2.	All concerned government agencies
3.	Online publishing

DOCUMENT REVISION HISTORY:

Version	Date	Author	Remarks
1.0	2017	Governance & Standards	Creation of document

Table of Content

1 INTRODUCTION

With the prevalence of the Internet, government agencies have to provide online access to information and e-services for the public. Government agencies' websites and web applications, whether outsourced or carryout internally, need to maintain the quality and security of the information and e-services provided to the public.

This policy provides direction to government agencies on maintaining websites and on the adoption of cloud computing services (hosting).

2 PURPOSE

The purpose of this Policy is to:

- Ensure government agencies have a trusted, reliable and secured web presence to the public (citizens, residents and commercial establishments).
- Facilitate a managed and coordinated adoption of cloud computing services.

2.1 SCOPE OF APPLICABILITY

This policy applies to:

- Government agencies' websites and web applications maintained either on the agencies' network or with a third-party (external) hosting provider, and to internal or third-party developers responsible for building or maintaining agencies' websites and web applications.
- Entities/establishments (government owned, or private) engaged in managing sensitive government data and information.

This policy replaces the existing "ITA.4.1 Website Policy" published and circulated to government agencies thru ITA circular number 1/2012 on April 23, 2012.

2.2 DEFINITIONS

Website: A website is a collection of related web pages, including multimedia content, typically identified with a common domain name, and published on at least one web server. A website may be accessible via a public Internet Protocol (IP) network, such as the Internet, or a private local area network (LAN), by referencing a uniform resource locator (URL) that identifies the site.

Web Portal: A Web portal is most often a specially designed web site that brings information together from diverse sources in a uniform way. Usually, each information source gets its dedicated area on the page for displaying information (a portlet); often, the user can configure which ones to display.

Web Application: web application or web app is a client–server software application in which the client (or user interface) runs in a web browser.

Mobile Application: mobile application software or mobile app is an application software designed to run on mobile devices such as smartphones and tablet computers. Mobile apps often stand in contrast to desktop applications that run on desktop computers, and with web applications which run in mobile web browsers rather than directly on the mobile device.

Cloud Computing: Cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services), which can be rapidly provisioned and released with minimal management effort. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in either privately owned, or third-party data centers that may be located far from the user–ranging in distance from across a city to across the world.

Cloud Service Models: Cloud-computing providers offer their services according to different models, of which the three standard models are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The NIST's definition of cloud computing defines the service models as follows:

- **Software as a Service (SaaS).** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- **Platform as a Service (PaaS).** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
- **Infrastructure as a Service (IaaS).** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

3 POLICY STATEMENTS

3.1 GOVERNMENT WEBSITES

1. Government agencies should:
   a. Implement and maintain a website to provide government information and e-services that are highly available and accessible to the public including the disabled.
   b. Consider W3C recommendations on One-Web-Approach while publishing their content on the web to ensure users get the same information and services regardless of which devices they use to access the Web Content.
   c. Implement quality controls to ensure that the content of information and e-services provided to the public are accurate and regularly updated.
   d. Implement security measures to ensure availability and integrity of the information and e-services provided to the public.
   e. Implement security measures to prevent the inappropriate disclosure of sensitive information.
   f. Ensure that the security measures are appropriate enough to satisfy Information and Information systems' classification.
   g. Identify and manage the risks associated with the publishing of information and e-services so that the public will have confidence and trust in the government.
   h. Obtain an independent security assessment of the government website or web application (including mobile applications); and before any major changes are applied; and all critical vulnerabilities are closed before publishing. Subsequently, the assessment should be carried out on annual basis.
2. Government agencies, that provide operationally critical information and e-services to the public, need to have continuity plans in place to deal with interruptions and disasters.
3. Government websites should:
   a. Minimally be in Arabic and English language.
   b. Be in the .om domain names (including all official public digital correspondences).
   c. Include privacy policy and website terms of use.
4. Government websites can provide link to other government websites and non-profit organizations. Links to private companies and individual's websites are not encouraged. Exceptions (if required) should be supported with proper business justification and approved by the competent authority at the agency.

3.2 PREPARE FOR DATA SECURITY

1. In all times Government Data shall be handled with due care.
2. Government agencies and any other entity – private or public – engaged in capturing, storing, managing government data shall establish adequate arrangement at their end to ensure proper handling of government data.

3. Government data shall be classified in accord of Royal Decree 118/2011. "Data Classification Guidelines" are published and available to assist entities in this regard.
4. Information Systems processing Government data should be classified according to "Information System Classification Guidelines" published by ITA.
5. Risks and the impact level associated with government data shall be assessed thoroughly (using Risk Management Framework), and the results should be documented and shared with the agencies' senior management, and their consent should be obtained on risk treatment approach.

3.3 Data Hosting and Cloud Services

1. Government agencies may adopt and use hosting and cloud services subject to business requirements and only after issues of security and data privacy have been identified and mitigated against.
2. Government agencies need to be aware of their privacy and data security obligations when transferring personal or government sensitive information into any cloud environment. If privacy issues cannot be adequately addressed, it may not be appropriate to transfer such information into a cloud.
3. The total cost of acquisition, with an emphasis on shifting costs from capital to recurring expenditure, must be taken into consideration in the procurement or adoption of hosting and cloud services.
4. As a rule of thumb, government data should only be hosted/transacted/processed with in the geo boundaries of Sultanate of Oman.
    a. Exceptions (if required):
        i. Government agencies should justify their need for exception to; and seek approval from Cabinet of Ministers.
        ii. Private entities handling government data should seek approval from their respective regulators (like CBO and TRA).
5. Government data and information hosted/transacted/processed on cloud based infrastructure should be encrypted.
6. Government agencies' taking online payments must host their solutions with a hosting provider meeting PCI DSS compliance requirements.
7. Government agency's use of hosting and cloud services must adhere to relevant legislation associated with information management including issues of privacy, legal, records management, and any other applicable requirements, such as, copyright, financial, ownership and geo-location of data.
8. Government data and information hosted/transacted/processed on managed cloud based infrastructure remain strategic asset of government agency and requires appropriate contractual agreements be in place. Government data and information must not be stored in external repositories that do not have contractual agreements in place with the agency (e.g. Dropbox, OneDrive, Google Drive, etc.).

9. Government agencies engaging contracted service providers (hosting and cloud services) need to take appropriate contractual measures to ensure:
    a. Government sensitive/personal information is protected, and contracted services providers (and any subcontractors) do not authorize acts or practices that would breach the Information Privacy & Security, regardless of whether or not the provider (and any subcontractors) are based in Oman or overseas (in case exceptions have been granted for overseas).
    b. easy and smooth disengagement and transition of services in case agency is transitioning to a new cloud computing services provider or alternatively bringing the services back in-house.
    c. retrieval of all data, in case of disengagement, in formats approved by the agency.
10. Agencies need to take particular care to ensure they are able to enforce the provisions of the agreement, even when contracting offshore (with proper justification and approval).

4 Roles and Responsibilities

4.1 Policy Management

1 Creation and maintenance of this 'Website and Data Hosting' Policy is vested with the Information Technology Authority (ITA).

2 ITA has the overall responsibility for facilitating the implementation of this Policy and providing advice and guidance to all government agencies, and target audience.

4.2 Policy Implementation

1 All government agencies and owners and administrators of government agencies' websites are responsible for implementing, complying and reporting improvements in relation to this policy.

2 ITA will conduct policy compliance checks, and security assessments of government websites and published web applications on periodical basis.

5 Related References

Following documents/links may be relevant to this policy.

A. Royal Decree 118/2011 – Data Classification Scheme
B. Oman Data Privacy Law (Draft)
C. Oman eTransaction Law (Draft)
D. Data Classification Guidelines
E. Information Systems Classification Guidelines
F. Risk Management Framework
G. Cyber Security Guidelines