Policy Making and Assessment: Case Study of Bahrain Enterprise Architecture’s Policy & Standards in Information Technology (IT)

Harikrishnan Sugumaran
IT Governance Architect, eGovernment Authority, Bahrain
hsugumaran@ega.gov.bh

Dr. Zakareya Ahmed Al Khaja
VICE CEO, eGovernment Authority, Bahrain
zahmed@ega.gov.bh

ABSTRACT

Building on the believe that there exists a positive correlation between the desired level of e-government capability and maturity and the required level of policy architecture maturity, The eGovernment Authority (eGA) of the Kingdom of Bahrain embarked a eGovernment program aimed at improving service delivery to citizens through seamless integration and connected governance.

In order to ensure increased efficiency and effectiveness of e-Government, it is important that “Whole of Government” operates in a consistent, standardized and best practice driven manner. That’s where the journey for kingdom wide e-Government policies and standards initiates. Policies are formal documents that aim to guide the behavior of Government and the application of standards with the aim of achieving a desired outcome such as “safe IT environment” or “efficient usage of IT resources”. These standards establish uniform requirements for all Government entities with regards to current or planned organizational component (e.g. Policy Standards, Architecture Standards, Technology Standards, and Program Management Standards etc.).

This paper will describe the Policy and Standards project starting with definition of policy, principle, objectives and scope of the project, the approach taken to plan & assess, Architect, design, implement, govern. This paper demonstrate primarily on brief description about architecting the policy lifecycle framework, formation of Governance structure, Roles & Responsibility of each stakeholder to govern and it excludes the syndication approach, we leave to audience belonged government region’s business reengineering culture and practice.

During the policy lifecycle framework, a clear policy making and assessment view was established and concluded. This built a foundation to study and analyze the current state in the government entity and the international best practices are taken into consideration to set a direction to redefine the policy making and assessment process according to the government culture in the Kingdom of Bahrain which support and revolve across eGovernment strategy and
Bahrain vision 2030. This policy and standard exercise triggered to identify and redefine eight (8) different domains in the Information Communication Technology (ICT) arena which is internationally acclaimed.

**INTRODUCTION**

Government around the world are leveraging advances in Information and Communication Technologies (ICT) to enhance their services delivery mechanism so as to improve citizen satisfaction towards government as well as gain competitive advantage over other nations in attracting. In order to achieve this objective, eGA realized the need for a Kingdom-wide strategy and holistic guiding plans, and hence decided to design, develop and implement National Enterprise Architecture Framework (NEAF) for Kingdom of Bahrain. NEAF would help in managing complexity, Manage IT portfolio, **Policy making and Assessment**, deliver road map for changes, support business & IT budget prioritization etc. Different issue in any organization like legacy transformation, business changes, infrastructure renewal, Application renewal and Business IT alignment can be resolve by designing Enterprise Architecture.

This paper demonstrates the **Policy Making and Assessment** for better Public Administration in the Kingdom of Bahrain. The prime objective was to **study existing IT policies** in the government and propose appropriate policies required and making structure, governance model for the Kingdom of Bahrain. In today’s connected and e-enabled world, it is critical that all government entities across the Kingdom operates in a standardized way ensuring seamless real time access to required information for delivering government services without compromising on security and privacy aspects.

With the world as well as the Kingdom accelerating towards technology enabled electronic channels for providing government services; eGovernment has emerged as one of the key drivers and pathfinder for transforming government experience. eGovernment is no longer restricted to e-enabling government operations; instead it has matured to be a key enabler in the transformation journey of tomorrow’s government.

**What is ‘Policy’?**

A definite course or method of action selected (by government, institution, group or individual) from among alternatives and in the light of given conditions to guide and, usually, to determine present and future decisions.

A specific decision or set of decisions designed to carry out such a course of action.

Thus, it would be incumbent for us to have our preferred definition, that is:

*“Policy is a decision-making framework or course of action to achieve a desired effect or change.”* In the context of the public sector, policies support political purposes by Government or administrative directions by organizations in response to the changing world around them.
Policy can:

- Be broad and visionary.
- Set direction.
- Express standards, behaviours, and expectations to guide actions.
- Be a concept or stated position of intended outcomes.
- Be a statement of principle.
- Policies are distinct from procedures and guidelines, which are operational instructions or processes for applying a policy decision. Operational procedures interpret policy and define activities that must be carried out to implement the directions and goals set by policies. They are designed to achieve outputs. To reach consistent results, they place boundaries on how much individual discretion is permitted when interpreting policy.

Driving Principle

This paper intended to demonstrate the eGovernment authority (eGA) Kingdom of Bahrain case study of policy making and assessment. eGovernment authority studied across twenty eight (28) government entities through a National Enterprise Architecture Program to streamline the public administration particularly in the field of information communication technology to ensure the standards and processes. The Policies and Standards are, Key to improve efficiency in eGovernment by

- Enforcing efficient governance & compliance across eGovernment ecosystem
- Achieving standardized operating environment conforming to best practices
- Easier accomplishment of connected government paradigm
- Critical to National Level Governance and compliance

Hence it should be managed centrally as National Initiative, owned by the formed governance group, it ensures the active involvement of Information Communication Technology Governance Committee (ICTGC) and Supreme Committee of ICT (SCICT) of Kingdom of Bahrain, and it should be implemented and monitored across ministries and government entities.

Project Objective and Scope

Enterprise Architecture (EA) is practiced in many industries; private and public sectors. It is very important before embarking EA’s “Policy and Standards” project that the objectives to be achieved are defined clearly. As a trend EA could serve different objectives; in this the primary objective implies in this policy and standards project is to transform Kingdom’s e-Government environment to implement cross-government IT policies and standards designed in conformance with international best practices yet customized for catering to specific needs of the Kingdom.
The policies and standards will be enforced, managed and governed across all entities. In particular, this project is conceptualized to accomplish the following specific objectives

- To ensure “Whole of Government” operates in a consistent way
- To achieve **Consistent interaction** across entities facilitating
  - Easier integration possibility
  - Improved Interoperability
  - Improved efficiency and performance
  - Improved citizen centricity across eGovernment services
- To adopt and implement **Systematic Enforcement** mechanism
- To run eGovernment in **Secure, Best Practice Driven** yet agile manner
- Should develop **policies & standards**, educate entities, as well as monitor and report on compliance to Supreme Committee of Information Communication Technology (SCICT).

This project mainly demonstrates the cross government policies associated with IT and applicable to all government entities. And it excludes specific policies related to particular initiatives (e.g. interoperability, Green IT, Spatial Data etc.) and Government function related policies (e.g. Legal, HR, Financial, Administrative policies etc.)

**Illustrative Approach**

A comprehensive set of activities needs to be followed by government entities for empowering the policy making and assessment journey. At first, the eGA has laid out overall approach mechanism as illustrated in the below figure. Which is a stage wise approach mainly consist of plan, assess, architect, design, implement and govern along with cross government collaboration.

![Figure 1: Illustrative Approach](image)
Plan & Assess Stage

During the planning stage there are key major activities are undertaken by the team to analyses, study the current state in the government to derive a mechanism to address, there are many data points had been collected from the National Enterprise architecture initiative’s AS-IS Architecture artefacts and as well made a survey with key government entities in the kingdom. The primary activities includes

- Identify and assess exiting Policies and Standards
- Establish complete list of required policies and standards
- Establish priorities and implementation sequence
- Identify Stakeholders
- Establish communication plan

This paper try to elaborate primarily on the architecting and governance framework model and try to explain one cross government key policy been designed approved by the committee and implemented and educated. In order to achieve a quality policies and expertise available in the kingdom, hence this paper does not elaborate detailed information of each stages since it is more theoretical in nature and all government can use their own pragmatic approach which is commonly been played across the region. eGA has played an advisory role and handed over to the respective domain policies to the respective expertise government entities to design and follow the policy lifecycle framework.

Architect Stage

This is the key area where the real policy lifecycle framework, governance model has been formed and team has formed the below stated activities to drive forward.

1. Policy and Standards Lifecycle Framework
2. Governance Structure
3. Define Stakeholder Roles & Responsibilities
4. Policy Structure and Criteria
5. Policy Criteria Decision Tree
6. Policy Document Templates
1. Policy and Standards Lifecycle Framework

Operating policy and standards driven eGovernment is a journey. Hence understanding, managing and governing the lifecycle is critical. Conceptualization, development and implementation of policies and standards require multiple critical perspectives to be addressed... Awareness on overall need among government entity leadership, Management support from all government entities, Effective participation from key entities, Acceptance of ownership across governing bodies and decision authorities, Conformance of policies & standards integrated with review and audit cycle. Well defined and agreed Policy and Standards Lifecycle framework as exhibited in the below figure…

![Policy & Standards Lifecycle Framework](image)

**Figure 2 Policy & Standard Lifecycle Framework**

**Set and Refine Policies and Standards**
As stated earlier the eGovernment authority conducted a study in National Enterprise Architecture program the existing policies survey across the government entities based on it most entities in Kingdom of Bahrain operate in SILO in absence of centralized policies and standards. This ADHOC approach inhibits achieving secure, best practice driven yet agile and connected eGovernment …. 

- **Issues Identification**
  The study concluded that the below stated are identified key issues ….
a. Cross-Government policies and standards are **not available** in all entities
b. **37%** of entities have **No Documented Standards or Policies** across IT domains
c. **50%** of entities rely on in-house standards and policies (not based on international best practices)
d. Handful of suboptimal centralized policies (not based on international best practices)
e. **Only 19%** of the entities have
   i. adopted IT / eGov policies and standards
   ii. implemented systematic enforcement mechanisms

**Resultant Consequences** based on the survey are:-

a. **High degree of heterogeneity** in similar business operations
b. **Disconnected government** – hard to execute cross-government services
c. **Inconsistent end user experience** on eService delivery
d. **Insecure, inflexible, vulnerable** Government ICT environment
e. **Integration and Interoperability challenges** – consistently increasing with enormous disparity
f. **Lack of agility and higher cycle time** in eGovernment operation
g. **Increased risk of underperforming** eGovernment systems

- **Agenda Setting**
Hence eGA set to refine policy standards as internationally acclaimed primarily in eight (8) domains in the Information Communication Technology (ICT) filed. Those are mainly as stated below each domain which consists of a set of policies in its basket and it has been prioritized by setting up criteria based on business value, security & operational importance.

1. Information Security Policies
2. ICT Environment Management Policies
3. IT Sourcing Policies
4. IT Development Policies
5. IT Deployment Policies
6. IT Usage Policies
7. eGovernment website & Social Media Policies
8. Information & Data Management Policies

2. **Governance Structure**
The primary governance structure main objective is to ensure development common policy framework and understanding that will enable improving the ICT maturity and adoption in Bahrain.
The group is responsible for overall policy planning, development and oversight, including reviewing changing requirements, establishing standard policies and guidelines and providing directional input to government entities.

Through the group, the leadership at each government entity will guide its implementation.

The policy Governance model primarily developed to enable the following

<table>
<thead>
<tr>
<th>Common Policy Framework</th>
<th>Citizen Charter Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>To strive towards an integrated and connected government through the development of common policies across all Government Ministries and Agencies.</td>
<td>To ensure citizen centricity of service delivery through the development and implementation of appropriate policies that enhances citizen confidence.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Program Management Framework</th>
<th>Awareness</th>
</tr>
</thead>
<tbody>
<tr>
<td>To provide an institutional mechanism responsible for coordinating and monitoring the implementation of the policies.</td>
<td>To ensure that there is enough awareness of the policies that are developed and implemented and the benefits are communicated to all stakeholders.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Monitoring and Evaluation</th>
<th>Capacity Building and Change Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>To monitor the level of compliance to the policies with an objective that they enhance citizen satisfaction and government transformation.</td>
<td>To ensure capacity development and skills by facilitating trainings and providing support in change management.</td>
</tr>
</tbody>
</table>

Based on the leading practices and rationale of independent working unit the following conceptual governance framework is formed for managing Policy Development, Implementation and Maintenance.

The Governance Structure comprises of the following sub-entities

1. Advisory Body
2. Lead Agency
3. Execution Units
4. Working Committees / Groups

5. Independent Working Groups

Advisory Body:
ICT Governance committee established in year 2011 to oversee and act as an advisory board in respect to Information Communication Technology related activities. It consist of the key members from different government entities like eGovernment Authority, Chief Informatics Organization (CIO), Ministry of Education (MOE), Deputy Prime Minister Office (DPMO), Economic Development Board (EDB), Ministry Of Industry and Commerce (MOIC), Ministry of Finance (MOF), University of Bahrain (UOB). In respect to policy drive in the country each member of committee has individual role to play according their Line of Business

Lead Agency:
As an organization that has a key role to play in the eGovernance Initiatives in Bahrain, eGA & Chief Informatics Organization (CIO) handle the role of a lead agency to ensure development and adoption of IT Policies and Procedures in Bahrain. These entities will provide for budgets, administrative requirements and personnel as required for the development of IT Policies and Procedures. Apart from organizational support, these entities will work with the ICTGC to have a final say in the approval of these policies and procedures.
**Execution Unit:**
Established under respective expert government entity, it takes the lead role to form a core team of individuals to participate in development, approval and revision of policies and procedures, etc. It also coordinates with the different stakeholders involved in policy development and roll-out process.

**Working committee or Groups:**
These are several specialist groups that provide specific functional and technical inputs into the policy development and implementation process. Usually these groups comprise of experts from various government agencies and ministries.

**Independent Groups:**
These are usually pool of expert outside the working groups comprising of individual experts / consulting firms for specific areas of contribution. (*Consulting firm like Booz, Wipro are contributed*)

**Governance Structure Relationship:** The below figure exhibits the relationship of each group how it interact and work together.

3. Define Stakeholder Roles & Responsibilities

   **Lead Agency:**
   - Direct, oversee and support the development, adoption and implementation of IT Policies.
   - Prioritize policy development effort based on the requirements of country level and ministry level ICT projects based on eGovernment strategy.
• Secure funding from ministry of finance for policy development and implementation projects.
• Monitor the progress of all approved policy and procedures to assure successful implementations.
• Direct, oversee and support the development, adoption and implementation of IT Policies
• Prioritize policy development effort based on the requirements of country level and ministry level ICT projects based on eGovernment strategy.
• Perform post implementation reviews and outcomes for each of the policy area based on agreed criteria with ministries and other agencies
• Approval of changes to the policies and procedures.
• Facilitate and support implementation activities at individual ministry / agency to ensure they are aligned to intended policy objectives.
• Ensure Policy Compliance requirements are understood, there is an awareness of risk and residual risks if any are understood and managed respective ministries
• Create synergies between ministries and agencies by enabling common set of policy framework and procedures.

Execution Unit:

• Manage the Policy Development and Implementation lifecycle and provide the technical expertise for development of IT Policies.
• Coordinate with the ministries to understand the specific inputs that need to be incorporated into the policy statements
• Drive the policy roll-out process by working closely with ministry nominated “Working Group Members”
• Identify areas of common requirements among participating ministries and agencies.
• Work across ministries to determine ownership for policy implementation

Working committee or Groups:

• Provide interface and Incremental construction of policies to make them applicable and specific to a particular ministries

• Provide inputs into developing specifications and composition of how these policies and procedures can be applicable in the context of a given ministry or an agency.

• Examine and consider existing processes and policies to enable seamless implementation
• Represents individual ministries on specific issues relating to policy development and implementation

4. Policy Structure and Criteria

Categories of government wide guidance (see Appendix 1 for additional information about these categories):

- Government IT Policies articulate the government’s values, principles, strategies, and positions relative to a broad IT topic. They are designed to guide organizational and individual behavior and decision making. They are concise, high-level, and independent of a given technology. Government IT policies are mandatory. All new or substantially revised policies, once approved by the ICTGC, will be submitted to each Government entity Audit for inclusion in the online Standard Practice Guide.
  Examples: Information Technology Networks Information Security Policy
- Government IT standards specify requirements for becoming compliant with government IT policies, other government policies, as well as applicable laws and regulations. Standards may include technical specifications. Standards are mandatory.
  Examples: IP Address Standards
- Government IT guidelines provide guidance and best practices relative to a particular IT topic. They may accompany, interpret, or provide guidance for implementing IT policies, other entity policies, or applicable laws and regulations. IT guidelines are not mandatory.
  Examples: Privacy and Retention of Security Logs
- IT Procedures document “how to” accomplish specific IT tasks or use IT services. These procedures may be localized to reflect the practices or requirements of a specific unit.

5. Policy Criteria Decision Tree

An IT Policy Decision Matrix and Decision Tree flow chart are available as planning guides and process reminders for policy development working groups. Both are based on the process flow described below.

IT Policy Decision Matrix (Appendix 2) & IT Policy Decision Tree Flow Chart (Appendix 3)

During the Planning and Initiation step of the policy life cycle process, the need for new or updated guidance may be triggered by various issues such as:

1. Laws, regulations or best practices which require new or updated guidance
2. Implementation of IT services or new technologies that require new or updated policies
3. Risk assessment, audits, and/or reviews of existing policies/guidance that reveal inconsistencies or gaps
4. Operational issues that require clarification of government entity’s position.

The planning process involves stepping through a list of questions to determine whether there is a compelling need for a guidance effort and, if so, what type of guidance (policy, standard, and guideline) needs to be created.

Questions and suggestions for relevant decisions are listed below.

1. **What are the consequences/risks of not having documented guidance covering this topic?**
   a) Is there a legal requirement to have documented guidance?
   b) Are there operational issues that require clear statement of direction?
   c) Is there new technology (such as cloud computing) that requires entity-wide guidance?
   d) Will documenting (and implementing) this guidance mitigates risks?

   *If the answer to any of the above is “yes,” documented guidance may be necessary.*

2. **What are the consequences/risks of having documented guidance covering this topic?**
   a) Is this guidance implementable?
      Does this guidance represent a strategy that we would like department to plan for, although it may not be currently implementable?
   b) Is there an existing policy that already addresses this topic?
   c) Does the proposed guidance contradict (explicitly or implicitly) current government policy, bylaw, or other laws/regulations?

   *If the guidance is necessary but not implementable across the government within a reasonable time frame, starting with guidelines (rather than a policy) is preferable. If there is a contradiction or inconsistency between the proposed guidance and existing policies or laws, further analysis is necessary with the participation of appropriate stakeholders to determine how to handle. An existing policy may be obsolete or substantially out-of-date; therefore, updating or expiring the existing policy may be the appropriate option.*

3. **Should this guidance be mandatory? Is it technology dependent?**
   a) Is there a decree / law requiring the government entity to follow this?
   b) Is there a contractual obligation for the government entity to follow this?
   c) Is there another reason why this should be mandatory?
   d) Will this guideline change when new technology is implemented?

   What part of the guidance is technology-dependent and what part can be stated as a general policy?

   *If the guidance is mandatory, implementable, and applicable across the government entity, and technology-independent, it should be stated as a policy. If it is mandatory, implementable, and*
applicable across the government entity, but specific to a particular technology, it should be stated as a standard. Another option is to create a combination of a short, high-level policy statement, and a detailed, technology-dependent standard.

4. **Can the essence of this guidance be summarized in no more than one page?**
   Short, high-level policy statements will typically be documented as a policy. More detailed documentation can be provided as standards, guidelines, or procedures. If the guidance cannot be summarized succinctly, and an umbrella policy does not exist, it may need to be represented as a combination of a policy and guidelines or standards.

5. **How often do policies and related guidance need to be reviewed in order to stay current and applicable?**
   Policies and related guidance should be reviewed annually at a minimum to ensure that policies are meeting legal and regulatory obligations, best practices, and keeping up with technological change.

6. **Are policy exemptions or exceptions allowed?**
   Exemptions to policies and related guidance are generally not allowed. If an exemption is necessary, then the requesting party must comply with the policy exception process.

7. **What determines whether a policy is entity-wide or department-level?**
   a) Should this guidance apply entity-wide to all users of government information resources?
   b) Should this guidance apply entity-wide to all IT providers?
   *These questions do not determine the category (policy, guideline, standard) but rather the scope for applicability.*

6. **Policy Document Templates**
   The team has come up with a detailed standard format to develop policies across the government entities. This minimizes the effort and standardizes the way of drafting the policy. This template has to be reviewed and updated in periodical manner.

   **Policy Statement**
   <<This section will contain the actual policy statement>>

   **Reason for the Policy**
   <<This section will describe the need and rational for developing the policy along with target objectives and potential benefits envisioned behind policy development effort>>

   **Applicability**
   <<This section will call out the applicability of the policy along with exceptions (if any)>>
Entities Affected by this Policy
<<This section will provide the overall impact of implementing this policy in terms of affected ministries and government entities>>

Who Should Read this Policy
<<Identifies the target audience for this policy>>

Responsibilities
<<This section will detail out the responsibilities for each stakeholder involved in execution / implementation / change of this policy. Along with responsibilities, overall ownership of the policy will also be called out in this section. Responsibility of each stakeholder will be described in separate sections and usage of itemized bullet points will be preferred for clear understanding>>

<Stakeholder Name>
<Stakeholder Name>

Guidelines and Procedures
<<This section will document / reference all guidelines and specific procedures which will need to be followed while executing / implementing this policy. For example, this section will describe the recommended involvement mechanism of required stakeholders or may refer to specific procedure to be adhered. >>

Principles
<<Most of the times, a policy is based on certain driving principles. This section will document the principles (if any) on which this policy is founded. The principles mentioned here must reflect complete concurrence and validate the contents in Section – Reason for the Policy. >>

Policy Monitoring and Evaluation
<<This section will describe the governance and management perspective of the policy. Policy monitoring subsection will illustrate how the implementation / adherence / conformance of the policy will be monitored including but not limited to recommended metrics. On the other hand, policy evaluation subsection will highlight the ownership and evaluation criteria and associated mechanisms. >>

Summary of Design, Implement & Monitor
Design and implement stage has been executed in phased or iterative approach due to syndication is time consuming and getting approval and implement in government culture is a very challenging task. These below are major activities are been involved by the execution team.

• Develop Policies using iterative model.
• Develop missing standards / refine existing standards.
• Obtain approval from relevant stakeholders through review and feedback

Piloting policy has been designed by expert team in a shorter duration; however as assumed the syndication has taken six months to finalize and approve by committee. Hence the design, implement and review stages will be executed as per planed stage through multiple iterative phased approach by key government entities and monitor by centrally.

CONCLUSION

In this paper, the planning and architecting the policy lifecycle framework, policy governance of initiative was discussed. Starting with objectives and scope of the initiative, the illustrative approaches taken into consider to develop the policy lifecycle framework, governance model to design and implement were discussed in detail. This policy and standards initiative is one among the key objective of National Enterprise Architecture to design to have a decision-making framework in the Kingdom. The policies will be designed and developed by iterative and phased approach in upcoming years by key government entities in the Kingdom and monitored centrally as per governance model to achieve and realize the “Whole of Government” objective, easier integration, improved interoperability, efficiency and performance across eGovernment services.
References

ICT policies and standards support the strategic directions of the ... These policies and standards apply to all Government of South Australia agencies and [http://dpc.sa.gov.au/policies-standards-and-guidelines]


Singapore can capture global opportunities in the ICT space ... develop an external wing; and (c) Policy and Government Ecosystem Thrust..... Is a major IT initiative that integrates the four major processes of a building project life cycle [https://www.mti.gov.sg/ResearchRoom/Documents/app.mti.gov.sg/data/pages/507/doc/ERC_STS_ICT_MainReport.pdf]


http://www.pmi.org/Knowledge-Center/Knowledge-Shelf/~media/PDF/Knowledge-Shelf/Pratt_2011.ashx

http://web.up.ac.za/sitefiles/File/Quality%20posters/Policy%20life%20cycle%20summary.pdf

## Appendix1: Policy Structure and Definitions

<table>
<thead>
<tr>
<th>Category</th>
<th>Purpose</th>
<th>Applicability</th>
<th>Approval Authority</th>
<th>Communications Approach</th>
<th>Frequency of Change</th>
<th>Other Characteristics and Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government IT Policies</td>
<td>• Have broad application throughout the government&lt;br&gt;• Articulate government’s values, principles, strategies, and positions&lt;br&gt;• Guide institutional decisions and direct individual behavior&lt;br&gt;• Support and enhance government’s mission&lt;br&gt;• Clarify requirements and exceptions&lt;br&gt;Interpret and help comply with laws and regulations&lt;br&gt;• Help manage institutional risk&lt;br&gt;Help promote operational efficiency&lt;br&gt;• Support and enhance government’s mission&lt;br&gt;• Clarify requirements and exceptions&lt;br&gt;Interpret and help comply with laws and regulations&lt;br&gt;• Help manage institutional risk&lt;br&gt;Help promote operational efficiency&lt;br&gt;• Interpret and help comply with laws and regulations&lt;br&gt;• Help manage institutional risk&lt;br&gt;Help promote operational efficiency</td>
<td>• Government-wide, all entities&lt;br&gt;• Typically apply to all users of Government information resources</td>
<td>ICTGC executives</td>
<td>Formally published through decree Web version published</td>
<td>Revisit annually</td>
<td>- Mandatory&lt;br&gt;- Independent of specific technologies&lt;br&gt;- Short, concise, clear&lt;br&gt;- Must be implementable and enforceable&lt;br&gt;- Consequences of non-compliance are typically provided&lt;br&gt;- Accountability for implementation must be specified&lt;br&gt;- Includes definition of terms (that are consistent across policies)&lt;br&gt;- Template</td>
</tr>
<tr>
<td>Government IT Guidelines</td>
<td>• Provide guidance and best practices relative to a particular IT topic&lt;br&gt;• May accompany, interpret, or provide guidance for implementing IT policies or policy aspects</td>
<td>Government wide</td>
<td>IT process owner for a given topic</td>
<td>Web version published at Government policy site</td>
<td>Revisit annually</td>
<td>- Not-mandatory, may provide alternative approaches&lt;br&gt;- May depend on specific technologies&lt;br&gt;- Generally high-level – do not include step-by-step process&lt;br&gt;- Typically reference a parent policy&lt;br&gt;- Template</td>
</tr>
</tbody>
</table>
## Policy Structure and Definitions

<table>
<thead>
<tr>
<th>Category</th>
<th>Purpose</th>
<th>Applicability</th>
<th>Approval Authority</th>
<th>Communications Approach</th>
<th>Frequency of Change</th>
<th>Other Characteristics and Notes</th>
</tr>
</thead>
</table>
| **Government IT Standards**     | • May accompany, interpret, or specify requirements for implementing IT policies or policy aspects  
                                 | • Serve to accomplish compliance or risk mitigation  
                                 | • May interpret laws and regulations  
                                 | • May specify rules for using a specific IT service | Government-wide (for a given topic)  
                                 | • IT process owner for a given topic or IT service provider | Web version published at government policy site | Revisit annually | • Mandatory  
                                 |                                                                           |                                            |                                               |                     |                                   |                                |
| **Procedures**                  | • Detailed step-by-step instructions  
                                 | • May implement policies or guidelines酿造 | As stated  
                                 | Applicable IT service provider | Posted at appropriate web site | Revisit annually | Must be consistent with IT policies and applicable standards |
| **Entity wise IT Policies, Guidelines, or Standards** | As defined above when unique entity-level requirements exist.  
                                 | Entity-wide (Health System)  
                                 | Applicable Entity authority | Posted at appropriate web site |                                      |                       |                                |
| **Department -Level IT Policies, Guidelines, or Standards** | As defined above when unique development-level requirements exist. For example, CIO’s Operation department has developed security policies that are more detailed than entity-wide policies.  
                                 | Department-wide  
                                 | Applicable entity authority | Posted at appropriate web site |                                      |                       |                                |
|                                 | • Needed only when entity-level unique situations need special handling  
                                 | • Consistent with entity policies but may be more restrictive |                                      |                                               |                     |                                |
Appendix 2: Policy Decision Matrix

Overview
This document outlines the decision points to determine if a policy, standard, or guideline is required.

Prerequisites
If the answer to any of the following is “yes”, then continue with the questions to determine what kind of documented guidance may be necessary.

1. Is there a legal requirement to have documented guidance?
2. Are there operational issues that require clear statement of direction or policy?
3. Is there new technology (such as cloud computing) that requires entity-wide guidance?
4. Will risks be mitigated by documenting (and implementing) this guidance?

<table>
<thead>
<tr>
<th>Criteria</th>
<th>If Yes</th>
<th>If No</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Is it implementable across the Entity?</td>
<td>Continue to #2</td>
<td>Create a Guideline</td>
</tr>
<tr>
<td>2. Is it compliant with existing policies or laws?</td>
<td>Continue to #3</td>
<td>Conduct further analysis with participation of appropriate stakeholders to determine how to handle</td>
</tr>
<tr>
<td>3. Is it applicable across the Entity?</td>
<td>Continue to #4</td>
<td>Skip to #9</td>
</tr>
<tr>
<td>4. Can it stand more than 1 year without review?</td>
<td>Continue to #5</td>
<td>Skip to #9</td>
</tr>
<tr>
<td>5. Would there be only a low number of exceptions?</td>
<td>Continue to #6</td>
<td>Skip to #9</td>
</tr>
<tr>
<td>6. Is it independent of a specific technology?</td>
<td>Continue to #7</td>
<td>Create a Standard or Create a high-level Policy and a Detailed Technology-dependent Standard</td>
</tr>
<tr>
<td>7. Does an umbrella policy not exist?</td>
<td>Continue to #8</td>
<td>Use the umbrella Policy and Create detailed Standard(s), Guideline(s), or Procedure(s)</td>
</tr>
<tr>
<td>8. Can it be summarized in approximately one page?</td>
<td>Create a Policy and Detailed Standard(s), Guideline(s), or Procedures, if needed</td>
<td>Create a high level Policy and A combination of Standard(s) and/or Guideline(s)</td>
</tr>
<tr>
<td>9. Is it mandatory?</td>
<td>Create a Standard</td>
<td>Create a Guideline</td>
</tr>
</tbody>
</table>

Appendix 3: Policy Decision Flow Chart

Start
(Prerequisite met)

1. Implementable across Government entity
   - Yes
   - Further Analysis
   - No
      - Guideline

2. Compliance w/ Policy & law
   - Yes
   - 3. Applicable across government
   - No
      - Guideline

3. Applicable across government
   - Yes
   - 4. Stand > 1 year w/ out review
      - Yes
      - 5. Low # of exceptions
         - Yes
         - 6. Technology independent?
            - Yes
            - 7. Umbrella policy does NOT exist
               - Yes
               - 8. Summarized in one page
                  - Yes
                  - End Process
                  - No
                  - Detailed technology dependent, standard

5. Low # of exceptions
   - No
   - Standard

6. Technology independent?
   - Yes
   - Hi-level Policy

7. Umbrella policy does NOT exist
   - No
   - Umbrella Policy

8. Summarized in one page
   - No
   - Detailed documented standard(s), guideline(s), or Procedure(s)

9. Mandatory
   - Yes
      - Standard
      - Hi-level Policy
      - Umbrella Policy
      - End Process
   - No
      - Guideline

Appendix 4: Policy domain and proposed policy

1. Information Security Domain
   1. National Information Security Policy
   2. Government Wide Access Control Policy
   3. Network Security Policy
   4. Electronic Messaging Communication Security Policy
   5. National IT Asset and Risk Management Policy
   6. IT Security Incident Response Policy
   7. Physical and Environmental Security Policy
   8. Government Staff IT Security Policy
   9. Identity and Access Management Policy
   10. Policy for prevention, detection, removal and reporting of malicious software’s
   11. IT Security Policy for remote access
   12. Small Office / Home Office Security Policy
   13. Password Policy
   14. Firewall Security Policy
   15. Public Key Encryption (PKE) Policy
   16. Policy to safeguard information on portable computing and storage devices
   17. Lost or Stolen Electronic Device Policy
   18. Security Control policies for Government Information Systems

2. IT Environment Management Domain
   19. Archiving and Records Management Policy
   20. Electronic Document Management Policy
   21. Project Management Policy
   22. Common Operating Environment Policy
   23. Disaster Recovery Policy
   24. Email usage and Management Policy
   25. IT Portfolio Management Policy
   26. IT Acquisition / Investment Policy
   27. IT Products (COTS) Acquisition Policy
   28. Internal Audit Policy
   29. IT Service Management Policy
   30. Anti-Spam Policy

3. IT Sourcing Domain
   31. Sourcing policy for IT roles in government entities
   32. Policy on sourcing model
   33. Vendor Management Policy
   34. Strategic Partnership policy

4. IT Development Domain
   35. Open Source Software and Systems Policy
   36. Software Development Lifecycle Policy
5. IT Deployment Domain
37 Application Deployment Certification Policy
38 Infrastructure Deployment Certification Policy
39 Domain Name Management Policy
40 Hosting Location Policy
41 Remote Hosting Policy
42 Software Usage Policy

6. IT Usage Domain
43 Specific Electronic device & software usage policy
44 Wireless LAN (WLAN) Management Policy
45 Network Technology Usage Policy
46 Network Device Management Policy
47 Policy for use of Government owned ICT resources and infrastructure
48 IT System Accessibility and usability policy

7. eGovernment, Website and Social Media Related Domain
49 Government wide Social Media usage Policy
50 eGovernment appropriateness of content policy
51 eGovernment Comment Policy
52 eGovernment Disclaimer Policy
53 eGovernment Website general look and feel policy
54 eGovernment Internet Link Policy
55 eGovernment Privacy and Security Policy
56 eGovernment Acceptable use policy
57 Policy on open standards for eGovernment

8. Information and Data Management Domain
58 Information Privacy policy
59 Data accessibility policy
60 Government Data Availability policy
61 Open Data Policy
62 Data Sharing Policy
63 Data Storage and information lifetime policy
64 Data backup policy
65 Waiver Policy