STATE OF ALABAMA

OFFICE OF INFORMATION TECHNOLOGY

STANDARD 101S1: IT Governance Documents

VERSION NUMBER	Standard 101S1-01
VERSION DATE	December 31, 2018
STANDARD TITLE	Information Technology (IT) Governance Documents
GOVERNING POLICY	This standard is governed by Policy 101: IT Governance, regardless of revision, and is required for all IT governance documents published by the Office of Information Technology (OIT) for statewide use.
OBJECTIVE	The objective of this standard is to define the statewide IT governance document structure, content (roles, responsibilities, requirements, etc.), numbering, and naming conventions used by the OIT. Agencies are expected to document their policies and procedures but are not required to follow the approach described herein.
SUPPORTING DOCUMENTS	The following documents support this standard: • Policy 101: IT Governance
STANDARD	1. IT GOVERNANCE DOCUMENTS IT governance documents consist of policies supported by the standards, procedures, guidelines, templates, and forms that document the IT management program. Each of these document types are defined below. 1.1. Policies: Policies define the overall expression of management's intention on how IT controls should be implemented, maintained, and enforced. Policies are usually subject-specific, and define the specific responsibilities that must be met by the individual, by the agency, by the OIT, and by any other specified role.

The OIT's statewide policies are mandatory for all entities subject to the authority granted to the OIT by the State Legislature (as stated in the governing policy).

The security and privacy controls specified by the National Institute of Standards and Technology (NIST) in Special Publication (SP) 800-53 (and other referenced NIST documents) provide the basis for many of the statewide IT and security policies, standards, and guidelines.

NIST Special Publications are available here: https://csrc.nist.gov/publications/sp

Other governance documents (standards, guidelines, procedures, templates, and forms) are derived from, or are related to, the statewide policies as shown in the figure below.

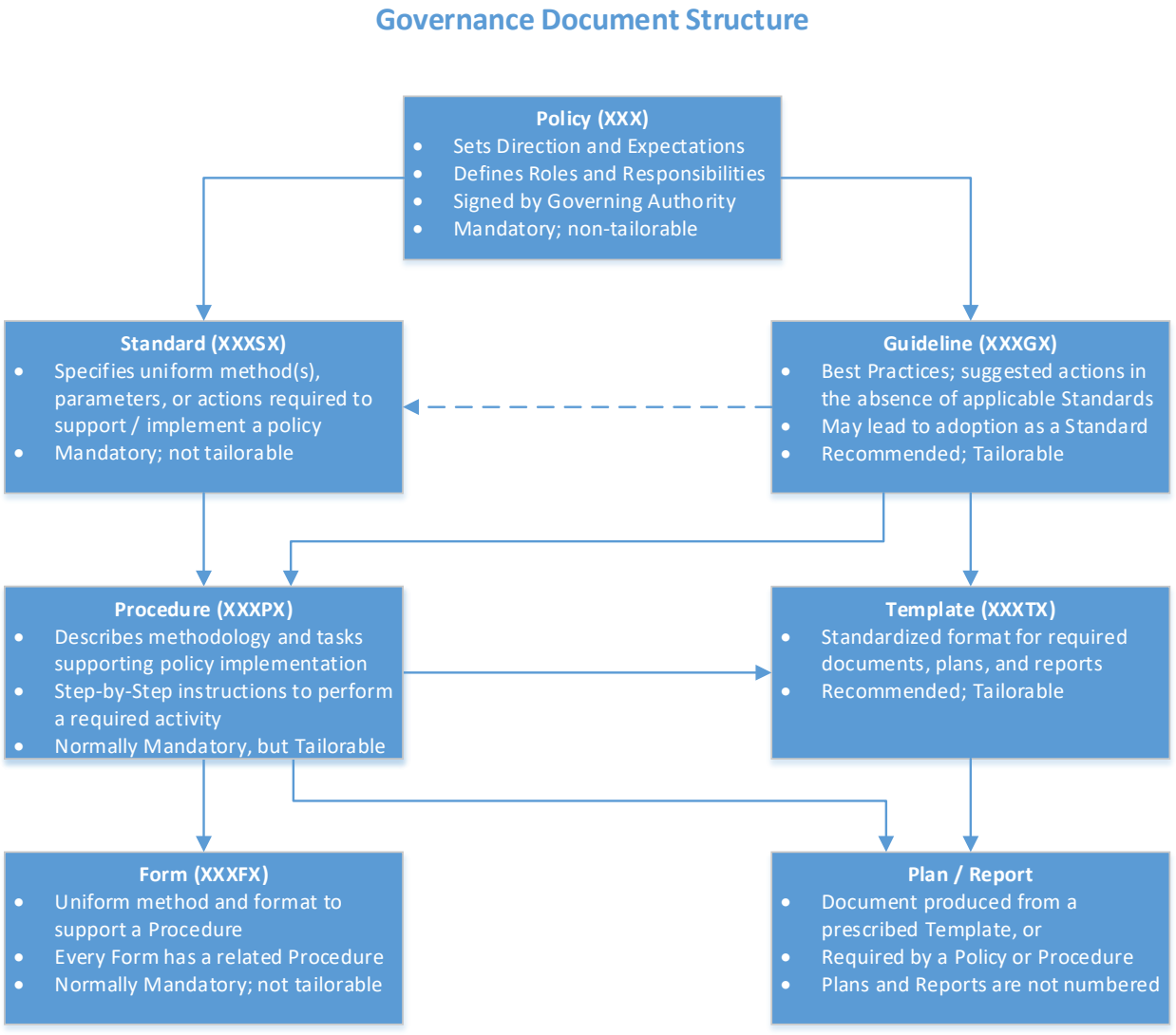

Figure 1: IT Governance Document Structure and Relationships

1.2. Standards:
Standards define system-specific or subject-specific requirements for implementing the corresponding policy. For example, a policy may address the high-level responsibilities for protecting systems from malicious code, whereas one or more standards would address the specific requirements for implementing anti-virus programs, anti-spam programs, etc. Standards are typically mandatory and may not be tailored; however, agencies may adapt a standard to suit agency-specific requirements provided agency requirements meet or exceed the minimum standards set forth in the OIT requirements.

Security standards may also be in the form of configuration checklists or benchmarks. These are based on or will reference publications from widely recognized sources of technical and security guidance including the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), the Center for Internet Security (CIS) Security Configuration Benchmarks, and NIST National Checklist Program (NCP) Repository.

DISA STIGs are available here: https://public.cyber.mil/stigs/

CIS Benchmarks are available here: https://www.cisecurity.org/cis-benchmarks/

NIST NCP Checklists are available here: https://nvd.nist.gov/ncp/repository

1.3. Procedures:
To implement a standard or a guideline may require one or more procedures. Procedures are step-by-step instructions or methods for performing a specific task or function. Creation of procedures is largely the responsibility of the implementing agency or entity responsible for performing the task. Statewide procedures (those published by the OIT) are normally mandatory, but may be tailored by the implementing agency. All tailoring decisions shall be documented by the agency.

1.4. Guidelines:
Guidelines are recommendations and best practices; not required, but implementation is strongly encouraged. Guidelines, when implemented or adopted, may become standards (if applicable).

1.5. Templates and Forms:
Procedures and guidelines may require (or request) submission of data or documentation and may specify a format for that submission using either a form or a template. Forms are normally mandatory and not tailorable. Templates are normally recommended and are tailorable.

1.6. Plans and Reports:
Plans and reports may be required by a policy or procedure or recommended in a guideline. They may be produced from templates where one is provided. Plans and reports are not numbered (all other documents types are numbered in accordance with the numbering standard described in the next section) and they may or may not be published (depending on purpose and content).

2. NUMBERING STANDARD (DOCUMENT SUBJECT CATEGORIES)

2.1. IT Governance documents are numbered by subject category as listed below:

100 – Information Technology (General)
200 – IT Planning, Budgeting, and Procurement
300 – IT System Lifecycle Management
400 – IT Project Governance
500 – IT Architecture
600 – Security and Privacy

2.2. The subject matter of each of these categories is described below.

100 –Information Technology (General)	Information Technology is intended to support agency missions and business needs. With this goal as a preconception, and in accordance with the authority and duties assigned to the OIT by State of Alabama Legislation, the OIT presents policies, procedures, standards, and guidelines for the management of state information resources.
200 - IT Planning, Budgeting, and Procurement	Important components of planning and budgeting consist of developing and maintaining a strategy for managing and maintaining information resources - a cyclical recurrence of reporting, planning, and executing.
300 - IT System Lifecycle Management	IT System Lifecycle Management governance and processes require the alignment of IT procurements with organization strategic goals, risk analysis of potential contractors and the products/services they provide, and risk analysis of alternative design implementations (with consideration for the full life cycle of costs and benefits).
400 - IT Project Governance	The OIT duty, as established in Alabama Code, to "establish and administer a structured system for review and approval of new information technology initiatives and projects, including business case, cost benefit analysis, and compatibility analysis," is expressed in the policies, procedures, and other resources created and maintained by the OIT Enterprise Project Management Office (EPMO).
500 - IT Architecture	The documents in this section provide reference architectures and service implementation guidance to support information system deployments. This includes solution-specific architectures, segmentation architectures, and other reference models that consider specific system, security, and privacy requirements.
600 - Security & Privacy	Protecting the confidentiality, integrity, and availability of information requires a risk-based approach that accounts for both the privacy and security aspects of data stewardship. Information security and privacy policies, standards, and guidelines are aimed at protecting information in a manner commensurate with the risk that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of such information.

3. DOCUMENT NAMING/NUMBERING CONVENTION

3.1. Policies:

Naming Standard: Policy NNN-nn [Title]
Where “NNN” is the policy number, based on document subject category number (as listed above or as subdivided)
Where “nn” is the version number; sequential, beginning with 01 for each policy
Where [Title] is a short (two or three word) description of the document contents or purpose

3.2. Standards:

Naming Standard: Standard NNNS#-nn [Title]
Where “NNN” matches the policy number to which the standard applies
Where S# is the standard number, where # is sequentially numbered beginning with 1
Where “nn” is the version number; sequential, beginning with 01 for each standard
Where [Title] is a short description of the document contents or purpose

3.3. Guidelines:

Naming Standard: Guideline NNNG#-nn [Title]
Where “NNN” matches the policy number to which the guideline applies
Where G# is the guideline number, where # is sequentially numbered beginning with 1
Where “nn” is the version number; sequential, beginning with 01 for each guideline
Where [Title] is a short description of the document contents or purpose

3.4. Procedures:

Naming Standard: Procedure NNNP#-nn [Title]
Where “NNN” matches the policy number to which the procedure applies
Where P# is the procedure number, where # is sequentially numbered beginning with 1
Where “nn” is the version number; sequential, beginning with 01 for each procedure
Where [Title] is a short description of the document contents or purpose

3.5. Templates:

Naming Standard: Template NNNT#-nn [Title]
Where “NNN” matches the policy number to which the template applies
Where T# is the template number, where # is sequentially numbered beginning with 1
Where “nn” is the version number; sequential, beginning with 01 for each template
Where [Title] is a short description of the document contents or purpose

3.6. Forms:

Naming Standard: Form NNNF#-nn [Title]
Where “NNN” matches the policy number to which the form applies
Where F# is the form number, where # is sequentially numbered beginning with 1
Where “nn” is the version number; sequential, beginning with 01 for each form
Where [Title] is a short description of the document contents or purpose

4. DOCUMENT REVISIONS

4.1. Major Changes:

Changes effecting the implementation of a rule, deletion of a rule, or the introduction of new rules will normally be considered a major change and will advance the version number of the document. Example: “Standard 101S1-02: IT Governance Documents” would indicate the second version (or first revision) of this document. Major changes shall be briefly described in the Document Change History table at the end of every document (except forms).

4.2. Minor Changes:

Corrections of grammar, spelling, and punctuation errors, format and style changes, and other changes not affecting the implementation or interpretation of any requirements are normally considered a minor change. Minor changes do not require document revision as described above. Minor changes may be made on published documents and annotated on the signed copy kept on file by the OIT office of Governance, Risk, and Compliance.

4.3. Recognizing Changes:

While the document version number will be revised with any major change, the version date will be revised with any major or minor change. When a published document is changed, the “Last Modified” date on the OIT website, IT Governance Library (http://oit.alabama.gov/governance-library/), will be updated. Always compare the version date printed on any locally-saved or printed copy with the last modified date from the OIT website to ensure you have the most recent document.

EFFECTIVE DATE	This standard shall be effective upon its approval by the Secretary of Information Technology, as evidenced by the signature of the Secretary being affixed hereto.
SUPERSEDES	This is the initial standard and does not supersede a previous version.

The undersigned, as Acting Secretary of Information Technology of the State of Alabama, exercising the power vested in that Office by the laws of this state, declares this standard to be adopted as of the 29th day of January, 2019.

Jim Purcell
Acting Secretary of Information Technology

DOCUMENT CHANGE HISTORY

Version	Version Date	Comments
101S1-01	12/31/2018	Initial version