Policies, Standards, and Procedures

Policies, standards, and procedures are necessary in order to effectively and efficiently guide the operations of any organization; they are especially necessary in order to ensure regulatory and procedural compliance in a large, multi-million-dollar program such as Maryland’s highly diversified and Statewide information technology operations.

Policies are first established in order to ensure consistent decisions and actions. Then standards are developed to guide compliance with established policies. Operational business rules, or procedures, are then developed to accomplish an organization’s purpose in a manner compliant with policy and in conformity with established standards.

The benefits of developing and strictly adhering to uniform policies and standards include:

- Systems have functional and technical compatibility.
- The technologies used to process applications will be relatively transparent to users.
- Application systems, data, access to pathways and graphical user interfaces will be standardized for the user – they look and work the same and are intuitive to a new user.
- All enterprise wide data is rationalized (i.e. Data elements mean the same thing from system to system and application to application because the data is uniformly defined throughout State systems.).
- Technologies and applications can be rapidly deployed and tailored for specific use because essential application code and data structures are replaceable and reproducible, not constantly reinvented.

IT standards define the ways in which a product performs. They provide a basis for reuse, internetworking, cooperation, and portability. Standards are necessary to promote transparent communications across the many systems operating in State government. State government is not unlike most information technology environments, which are heterogeneous, rather than homogeneous. This means that the environment is made up of hardware, software, and other components that represent a variety of standards, products, and vendors, rather than an enterprise view with common standards.

Standards are important in providing the rules by which information technology products interact with each other. They are essential in ensuring that systems can communicate, which is essential in evolving network-centric IT strategy. Standards such as network protocols and interfaces between applications allow systems on a variety of hardware and operating system platforms to share information and data.

It is critical that standards be established and maintained in order to accommodate existing technologies as well as emerging ones. The technology in many areas, such as desktop computing, is evolving rapidly and standards in these areas will need to be updated frequently as the technology changes. The standards in other areas, such as network protocols, may change more slowly but need to be reviewed and evaluated regularly.
A review of the 2001 Government Performance Project data indicated that the States which achieved the highest scores in information technology: Utah (A), Washington (A), Kansas (A-), Michigan (A-), Missouri (A-), and Virginia (A-), all have developed comprehensive and detailed policies and procedures governing their information technology tools and services.

While Maryland has developed some IT policies and standards, additional policies and standards must be developed in order to implement an enterprise architecture to ensure the delivery of standardized, quality information services to both State employees and the citizens of Maryland.

Policies and guidance will be developed in the following areas:

**Information Technology Investment Management**
This policy will dictate how State Departments, Agencies and Organizations will select (which projects get funded), control (ensure projects are developed to meet requirements and on-time and within budget), and evaluate (ensure deployed systems continue to meet mission requirements effectively and efficiently) their information technology projects. The guidance will include the development of IT master plans, development of IT process requests, and alignment of the IT investment process with the budget process. State Departments, Agencies and Organizations will identify the IT portfolio and determine the medium and large IT projects. Capital plans will be developed for all large projects, regardless of where the project is in its life cycle. The CIO will modify and implement the Federal Government Smart Practices In Capital Planning Program as its framework for Capital Planning. Capital Planning is defined as “a collective decision-making process for ensuring that IT investments integrate strategic planning, budget, procurement and the management of IT in support of agency or company business processes.”

**Enterprise Architecture**
A strategic information asset base which defines (1) the current business, the information necessary to operate the current business, the technologies necessary to support the current business operations; (2) the target business, the information necessary to operate the target business, the technologies necessary to support the target business operations; and (3) the transitional processes necessary to get from the current environment to the target environment.

**Systems Development Life Cycle**
Defines all actions, functions, or activities to be performed by State Departments, Agencies, and organizations in the defining, planning, acquiring, developing, testing, implementing, operating, maintaining, enhancing, and modifying information systems.
People Capability Maturity Model
A maturity framework that focuses on continuously improving the management and development of the human assets necessary to acquire, implement, and support an organization’s information technology assets.

Electronic Records Management
The management, retention and ultimate disposition of electronic records in accordance with regulatory records keeping and management requirements.

Shared Services
The participation of more than one business unit in the use of a resource for the purpose of making business applications easier, faster, more reliable, and more cost effective (e.g. net.work.Maryland).

Security
Defines the policies and procedures to ensure the confidentiality, integrity and availability of State computer applications. Areas include, but are not limited to: password usage, computer virus, disaster recovery, risk assessment, encryption, auditing standards, intellectual property protection, etc.

Technology Assistance for Individuals With Disabilities
Defines electronic equipment accessibility and the application/configuration of electronic office equipment in a manner that accommodates the functional limitations of individuals with disabilities in order to promote productivity.