Minnesota Enterprise Technical Architecture

Revision 2.02

Revision History

Document Revision History

Version	Date	Description
Release version 1.0	Feb 28, 2002	First release. Identical to Beta version 1.0b4
Release version 1.1	May 2003	Second release.
Release version 1.9	Sept. 30,2004	Third release. Most domains at 2.0
Release version 2.0	Jan. 14, 2005	Fourth release
Release version 2.01	May 19, 2006	Fifth release required for portal
Release version 2.02	Sept. 8, 2006	Minor release

Chapter Revision Table

Chapter	Chapter Title	Version
Preface	Preface	2.01
1	Conceptual Architecture	2.01
2	Network	2.02
3	Platform and Storage	2.01
4	Data & Records Management	2.02
5	Data Interchange	2.02
6	Application	2.01
7	Middleware	2.02
8	Presentation, Accessibility	2.02
9	Collaboration and Workflow Tools	2.01
10	Security	2.02
11	System Management & Reliability,	2.02
A	Lexicon	2.01

Table of Contents

Preface

Introduction

The rate of change in the business and administrative process of organizations is accelerating causing the cycle times allowed for implementing new service systems to decrease. Existing IT infrastructure often gets in the way of rapid change and may inhibit the state's ability to respond to these shrinking cycle times. Some of their aspects may be difficult to adapt to more demanding requirements. There is also a demand from policy-makers for the effective use of IT resources and the deployment of efficient systems.

To accommodate these trends, we establish this ***Minnesota Enterprise Technical Architecture***.

Charge

This reference document is created and maintained by the Minnesota Office of Enterprise Technology and describes principles, practices and standards to define an Enterprise Technical Architecture for information systems in the State Government of Minnesota.

Authorizing State Statute and Requirements

The Minnesota Office of Enterprise Technology is charged with establishing and maintaining a state information architecture as specified in Minnesota Statue, Chapter 16E.04 Subdivision 2 which states:

> **Responsibilities.** (a) In addition to other activities prescribed by law, the office shall carry out the duties set out in this subdivision.
>
> (b) The office shall develop and establish a state information architecture to ensure that further state agency development and purchase of information and communications systems, equipment, and services is designed to ensure that individual agency information systems complement and do not needlessly duplicate or conflict with the systems of other agencies. When state agencies have need for the same or similar public data, the commissioner, in coordination with the affected agencies, shall promote the most efficient and cost-effective method of producing and storing data for or sharing data between those agencies. The development of this information architecture must include the establishment of standards and guidelines to be followed by state agencies.
>
> (c) The office shall assist state agencies in the planning and management of information systems so that an individual information system reflects and supports the state agency's mission and the state's requirements and functions.
>
> (d) The office shall review agency requests for legislative appropriations for the development or purchase of information systems equipment or software.

> (e) The office shall review major purchases of information systems equipment to:
>
> > (1) ensure that the equipment follows the standards and guidelines of the state information architecture;
> >
> > (2) ensure that the equipment is consistent with the information management principles adopted by the information policy council;
> >
> > (3) evaluate whether the agency's proposed purchase reflects a cost-effective policy regarding volume purchasing; and
> >
> > (4) ensure that the equipment is consistent with other systems in other state agencies so that data can be shared among agencies, unless the office determines that the agency purchasing the equipment has special needs justifying the inconsistency.
>
> (f) The office shall review the operation of information systems by state agencies and provide advice and assistance to ensure that these systems are operated efficiently and continually meet the standards and guidelines established by the office. The standards and guidelines must emphasize uniformity that encourages information interchange, open systems environments, and portability of information whenever practicable and consistent with an agency's authority and chapter 13.
>
> (g) The office shall conduct a comprehensive review at least every three years of the information systems investments that have been made by state agencies and higher education institutions. The review must include recommendations on any information systems applications that could be provided in a more cost-beneficial manner by an outside source. The office must report the results of its review to the legislature and the governor.

Also, Minnesota Session Laws 2001, 1st Special Session, Chapter 10, Article 1, Section 12, Subdivision 3.e states:

> The office must establish the state information architecture under Minnesota Statutes, section 16E.04, subdivision 2, by March 1, 2002.

Compliance and Migration

Compliance: Systems and technology infrastructure implemented by Minnesota State government must be compliant with this enterprise architecture even though there may be some additional cost to the agency for initial implementation or ongoing maintenance. The additional effort and expense of a compliant implementation will be compensated by the ease of future integration, data sharing and interoperability. Compliance of new systems must be documented in each agency's *System Information Resource Management Plan*.

Migration of Existing Systems: Existing hardware and software systems that are not in compliance at the initial implementation of the Enterprise Architecture need not be immediately replaced, but should be brought into compliance as a part of their regular upgrade or conversion cycle. It is recognized that additional financial resources may be necessary to replace existing

systems with those more compliant to the Architecture

Exceptions to Compliance: Architectural exceptions will be handled on a case-by-case basis by an inter-agency Architectural Review Board. The agency requesting an exception must provide adequate evidence of business need with justification based on the benefit vs. the cost of non-compliance and the total cost of ownership from the point of view of the state as a whole.

Purpose

This technical architecture is established to describe technology components of the State's information infrastructure and their individual principles, practices and standards that are to be used to guide the development and delivery of all information systems services. The architecture will provide a reference so that various groups of government IT professionals have a consistent view of the information systems infrastructure and the methods that they employ to develop and deliver information systems services. The purpose of this Technical Architecture is:

1. To provide a framework and boundaries to create systems that are rapidly adaptable while also integrated and interoperable (when required) so that they provide for the sharing of components, subsystems, or other functionality.
2. To provide a well-defined platform upon which a wide variety of enterprise-wide applications and advanced electronic government services may be quickly deployed.
3. To provide a documented plan to illustrate to policy-makers that all agencies are creating new systems and migrating old systems in a universally consistent way.

The planning and management of the State's enterprise technical architecture must have a planned evolution that is governed across the enterprise. Architecture support and review structures within the Minnesota Office of Enterprise Technology will be used to ensure that the integrity of the architecture is maintained as systems and infrastructure are acquired, developed and enhanced. This will help to ensure that the various development projects being managed within the State do not attempt to make incompatible changes to the technical infrastructure.

Definition and Scope

The purpose of this reference document is to define an Enterprise-wide *Technical* Architecture for the State Government. For our purposes, the scope of the Enterprise in question is the Executive Branch—all of the cabinet-level and smaller agencies.

Enterprise Technical Architecture is defined as:

> *A logically consistent set of principles, practices, standards, and guidelines that are derived from business requirements and that guide the engineering of an organization's information systems and technical infrastructure.*

The Executive Branch of state government is made up of many agencies, each with a significantly different mission and constituency. It may not be thought appropriate to consider the en-

tire Executive Branch as a single enterprise in the commonly understood sense of information technology. However, there will be a need for applications and services that will draw upon the resources and information of multiple agencies. There will also be functionality needed within the systems of several agencies that would be more effective if shared with others or that drew upon methods already developed by others. Deployment of new systems that are in compliance with a common Technical Architecture will enable the implementation of new inter-agency applications and the delivery of a wide range of advanced electronic government services without the need for large-scale reconstruction of those systems.

The focus of this architectural specification is on those systems, subsystems, and components that will have or show a reasonable probability of having to share data, interoperate, or be consistent with the systems, subsystems, or components outside the agency. The architecture, design, and implementation of those systems, subsystems, or components that will not require any external interaction or consistency are left to the discretion of the agency so it may best effect its own operations.

The scope of this architecture does not include the upstream steps of Enterprise Business Architecture, which is the expression of the enterprise's key business strategies and their impact on business functions and process. Nor does it include a complete information architecture, which is the expression of the enterprise's information and how it is cataloged, classified and stored. There are some aspects of an information architecture in the Data and Records Management domain, but this is not meant to be a finished or complete information architecture. Those are areas of much larger effort that may be initiated later as needed or justified to support the Technical Architecture.

On the downstream side, the scope of this Technical Architecture does not include direct support for the creation of an application portfolio or construction of a specific set of implementation and migration plans. Though the usual path of a complete architectural effort for an enterprise includes a path through business architecture, information architecture, technical architecture, application portfolio and implementation/migration plans, the State Government breaks the path of that model since it is difficult to conceive of it as an integrated enterprise. However, the Technical Architecture can describe a set of building materials and construction standards that would allow the individual agencies to build constituency-specific applications and systems that would have a much higher degree of data sharing, interoperability where needed, and consistency of implementation that would all provide positive benefits for future state IT systems.

Target Audience

This Technical Architecture is developed as a reference and direction to guide the decisions and actions of the following:

- Agency information technology executives, primarily the Chief Information Officers or their equivalents within the State agencies
- Agency information technology architects, planners, project managers and developers
- Information Policy Council

It is also available to guide the decisions of IT executives, architects, planners and project managers within all other government or non-government entities that develop and deploy informa-

tion systems that need to communicate with or inter-operate with State government information systems.

Expansion of this architecture to include the Judicial and Legislative branches of state government would be the logical next step of the Enterprise Architecture process.

Method

A key driving factor of this enterprise architectural effort was to get a useful reference in place quickly primarily because it is much needed and long overdue. There is also a need to have some guidance in place to permit designers to be in step with or preferably ahead of some major upcoming Information Technology (IT) decisions. Discussions on enterprise architecture have occurred several times in the past at the higher conceptual levels. It was apparent that tolerance to continuing at that level was diminishing and there was a desire to provide useful guidance for development decisions.

In 2000, the Office of Enterprise Technology engaged Meta Group of Stamford, Connecticut to help with a technical architecture methodology. We have adapted that process, using a fast-path subset to get a technical architecture implemented. We were also able to draw upon the architectural work of several other states who had used the Meta process, as templates.

The fact that much of today's development methods are converging on fewer choices as superior technology and methods become visible and quickly adopted industry-wide allows us to dive down into the technical architecture level at a more rapid pace. We have adopted a project style of a "rapid prototype" to establish a first draft architectural reference that will satisfy the vast majority of development needs and demonstrate that real and sincere cooperative efforts are underway among the State agencies.

Various parts of the architectural reference will have different levels of detail depending upon how well established the technologies and methods in those areas are. Ongoing work to fill out those architectural domains that may be more ambiguous will always be underway to assure that the architecture will provide the guidance needed and that it will continually adapt as industry trends and operational environments evolve.

Process

An architectural definition process was launched by the Office of Enterprise Technology in the first half of 2000 with educational workshops and high-level discussions in order to understand the methodology to be used and to establish the business drivers for the Technical Architecture. An architectural design project to create and publish the Technical Architecture began in January 2001.

The architectural team consisted of two main groups: a Working Group and an Advisory Group. The Working Group was staffed by leading technical people from the various agencies and was expanded into several technical teams, which defined all of the details of the architecture. The Advisory Group was staffed by Chief Information Officers (CIO's) or equivalent of the leading agencies and sat in the position of an Architecture Review Board. They had the final say in the

definition and establishment of the Technical Architecture.

After release and publication of the first version of this reference in February 2002, the Architectural Review Board was established under the authority of the Information Policy Council and is empowered to periodically review and update this Technical Architecture to keep it current with industry practice and State needs. Numerous standing technical working groups are also established to provide assistance and technical guidance to the Review Board.

Structure

Architectural Levels

A Technical Architecture can be written at various model levels. At the highest level is the ***Direction model***. This sets the "target" that is used as the basis for assessing the value of the completed architecture. At this level we identify business goals, technical goals, principles, assumptions, constraints, key performance factors and perhaps technology trends. These are the business drivers that set the environment for the rest of the Technical Architecture.

The next level is the ***Conceptual Architecture model.*** This is guided by the Direction model and is where we consider various high-level computing alternatives, focusing on structures such as classic two, three or N-tier systems, client-server systems, or distributed networked systems. The Conceptual Architecture guides the scope of the contents of the various technical domains that are expanded in lower level models. The Conceptual model is described in the Conceptual Architecture chapter.

The underlying Domain architectures are described using Logical or Physical architecture models. The choice of layer will depend on the ability to proscribe specific physical systems or technologies across the entire enterprise. In some cases, because of the wide diversity of environments at the agencies, it may not be possible to establish physical layer standards.

The ***Logical Architecture*** facilitates the understanding of the issues that must be considered in the development of the physical system environment. The Logical architecture model is not sufficient or intended to be implemented directly. It is generic, intended to support the discussion and comparison of alternative solutions. By using the Logical model, it is possible to determine the degree to which existing systems conform. It is not a requirement that the Logical Architecture model be a generalization of all existing physical architectures, but it should provide a comprehensive plan for further physical information system development and evolution.

The ***Physical Architecture*** model is concerned with the implementing technologies. The physical model "specializes" and details the logical architecture to suit our particular physical information environment. Here we are specifically concerned with products, vendors, versions, configurations, performance and implementations. It is critical to establish "proof-of-concept" of the logical and physical architecture before expensive final commitments are made.

Document Structure

The ***Conceptual Architecture*** contains the high level values upon which all of the underlying

subsystem architectures are based. The individual ***Domain Architectures*** contain principles, practices and standards for specific areas of the Enterprise at either the Logical or Physical level.

Domain Section Structure

The architecture for each Domain is specified within a chapter. The Domain is specified in several parts:

1. **Purpose:** States the business rationale as to why this particular domain is specified.
2. **Scope:** Describes what parts of the architecture this particular domain covers
3. **Principles:**
    a) Describe fundamental truths at a high conceptual level.
    b) State ideas or concepts that frame and contribute to the understanding of technical topics contained in the section.
    c) Establish a basis from which to form further recommendations.
    d) Contain brief rationale and implication statements to justify its existence and explain its effect(s).
2. **Best Practices:**
    a) Serve to direct or guide the detailed design, selection, construction, implementation, deployment, support, or management of the architectural framework.
    b) Are based on the success story of one or more other clients, or the industry as a whole.
    c) Are of the nature, "If you're going to do it, this is the recommended way."
    d) Are desirable (as opposed to mandatory) when implementing new systems in house or specifying Request For Comment (RFC) items.
    e) Has a brief rationale to justify or explain its existence.
3. **Technologies, Components and Methods:**
    Within each domain there will be several technical component or practice groupings, each described by a table and some explanatory text. The table will list the general technologies, products or services to be used in new development projects, delineating the technology components that comprise the architectural guidelines or standards and their status. Formatting of each entry will indicate the compliance requirement.

Table Formatting:

Plain text: Guidelines — strongly recommended for interoperability and full compliance.

Bold underline: Standards — mandatory for compliance.

*****: Indicates that a guideline or standard is designated as an open system.

Definitions:

Transitional: those that are twilight, retired, or soon to be retired technologies, components and methods and should be discouraged from new implementations. This is not to imply that existing

systems need be retired or replaced immediately, but that the use of these products and services should not be extended in any future planning and development.

Current: those that are preferred or required and should be used when making design and implementation decisions.

Emerging: those that include near-term directions and options that need continued monitoring to find applicability within the State IT infrastructure. Included are technologies that are not yet fully production-worthy but are potential candidates for prototype implementations. Continued market acceptance and adaptation will likely move these solutions toward the growth phase of the lifecycle, and inclusion in the statewide architecture will become apparent.

Responsibility and References: what party or group is responsible for keeping this item updated as business needs or technology and industry trends evolve, and/or, a URL or other reference to a defining document or standards document that specifies detail for the technology, component or method.

1. Conceptual Architecture

Purpose

A principal design consideration of a technical infrastructure is to facilitate easy and rapid change. This change, driven by business requirements from the legislature and external trends, will increasingly be implemented across the enterprise and with external partners, not just within individual agencies. Accommodation of these rapid business changes is enabled by a well-designed technical infrastructure that is broader and more forward-looking than the immediate application requirements.

The Conceptual Architecture contains values and practices that represent the core business and technical ideas on which all the technical domain architectures are derived. These values guide the implementation of technology to meet business requirements and promote service sharing. They are the rules that guide investment and design to maximize the business benefit and the adaptability of the IT environment.

Scope

The Conceptual Architecture describes the top-level concepts of the entire Enterprise Technical Architecture. Values and practices listed here apply to all domains. Concepts that are focused on more specific areas of the technical architecture are in the applicable domain chapters.

Business Drivers

A Technical Architecture must be based upon an accepted set of business needs: the motivation factors and case for action. The following have been defined for the purposes of this Enterprise Technical Architecture:

1. **Appropriate government information and services will be accessible regardless of location, time, and method of access and group (e.g. language, culture, age and ability).**
2. **Access to information and services will be authenticated to the degree required by specific information and services. Information will be protected to the level required both internally and externally.**
3. **Coherent and navigable access will be provided across multiple points of interaction for government information and services spanning departments and other levels of government (i.e., "no wrong door").**
4. **Government information and services will quickly respond to the client's changing expectations**
5. **Government service levels and functionality, focused on citizen values, that are provided via technology improvements will be pursued providing there is no proportional impact relative to costs. Costs and quality will be considered as 'tradeoffs' to the citizen value equation.**

6. **Government will reduce the total cost of ownership of IT investments through the elimination of duplicate infrastructures or support services and the leveraging of economies of scale.**
7. **Government will increase attractiveness for business investment in the State to build stronger local economies.**

Values

These provide an expression of values to be used in making technical choices in all new development efforts. The order of these values does not imply priority.

1. **IT as state assets:** Information and applications technology are valued as state enterprise assets, managed by specified custodians on behalf of the citizens of Minnesota.

   Rationale

   - Information is the State's most important asset. Collecting data and assembling information is expensive. These can be used to enhance and accelerate decision-making, which often requires information beyond the borders of a single agency. Local and federal governments are dependent upon this information.

   Implication

   - There must be documentation and inventory of assets. There must be a consistent technical architecture or framework to share information and services. There must be sufficient security precautions and disaster recovery procedures. There must be a new way of thinking about ownership of information, i.e. data and information are a common asset rather than local property.

2. **Total cost of ownership design:** Systems will use a total cost of ownership model for technologies which balances the costs of development or purchase, support, disaster recovery, and retirement against the costs of flexibility, scalability, ease of use, risk of data loss, and reduction of integration complexity.

   Rationale

   - This allows agencies to make better choices to better manage state assets on an enterprise level. Deployed solutions will likely be superior. The IT environment will be simplified.

   Implication**:**

   - This may require larger funding requests up front in the early build or purchasing stage, which will be offset by longer-term savings.

3. **Mainstream technology use:** Production IT solutions must use industry-proven, mainstream technologies except in those areas where advanced higher-risk solutions provide a substantial benefit. Mainstream is defined to exclude advanced technologies not yet in general use and older technologies and systems that have outlived their effectiveness.

   Rationale

   - The state does not want to be on the leading edge for its core service systems. Risk will be minimized.

   Implication**:**

   - There will be an element of risk avoidance in constructing core production systems. We are generally not going to be early adopters of new technology. There must be a continual evaluation of old technology deployment to hasten its retirement.

4. **Interoperability and reusability:** Systems will be constructed with methods that substantially improve interoperability and the reusability of components.

   Rationale

   - Enables the development of new inter-agency applications and services.

   Implication:

   - Use multi-tier distributed component design. Provide the service of object request brokers.

5. **Open systems:** Design choices prioritized toward open systems will provide the State with the best ability to create adaptable, flexible and interoperable designs.

   Rationale

   - An open, vendor-neutral policy provides the flexibility and consistency that allows agencies to respond more quickly to changing business requirements.
   - This policy allows the state to choose from a variety of sources and select the most economical solution without impacting applications. It also supports implementation flexibility because technology components can be purchased from many vendors, insulating the state from unexpected changes in vendor strategies and capabilities.

   Implication:

   - Open standards do not exist for all parts of the architecture. Therefore, a combination of de facto industry standards, product standards, and open standards will be required in order to support a heterogeneous operating environment.
   - Open systems must be differentiated from proprietary systems throughout this architecture.

6. **Reduction of integration complexity:** The architecture must reduce integration complexity to the greatest extent possible.

   Rationale

   - Increases the ability of the enterprise to adapt and change.
   - Reduces product and support costs.

   Implication:

   - May reduce flexibility as a trade off toward interoperability.
   - May sacrifice performance and functionality in some instances.

7. **Scalability:** The underlying technology infrastructure and applications must be scalable in size, capacity, and functionality to meet changing business and technical requirements.

   Rationale:

   - Reduces total cost of ownership by reducing the amount of application and platform changes needed to respond to increasing or decreasing demand on the system.
   - Encourages reuse.
   - Leverages the continuing decline in hardware costs.

   Implication:

   - Scalability must be reviewed for both “upward” and “downward” capability.
   - May increase initial costs of development and deployment.
   - Will reduce some solution choices.

8. **Integrated reliability, availability, and maintainability:** All systems, subsystems, and components must be designed with the inclusion of reliability and maintainability as an integral part. Systems must contain high-availability features commensurate with business availability needs. An assessment of business recovery requirements is mandatory when acquiring, developing, enhancing, or outsourcing systems. Based on that assessment, appropriate disaster recovery and business continuity planning, design and testing must take place.

   Rationale

   - Citizens and businesses depend upon the availability of government information and services. To assure this, reliability and availability must be designed in from the beginning; they cannot be added afterward. The ability to manage and maintain all service resources must also be included in the design to assure availability

   Implication

   - Additional up-front design efforts, additional design expenses, built-in redundancies and rapid recovery facilities, integration with a common management system.

9. **Talent optimization:** System development and operational environments will be oriented towards a statewide consistency.

   Rationale

   - Programming and operations staff is the most difficult resource to acquire and the largest portion of any development or operations budget. Costs of training, education and ramp-up latency time, if staff migrates among the agencies, can be substantial if differing environments are maintained. The need to make the best use of available talent and provide the greatest career opportunities for state staff is critical to the success of rapid system deployment and technical talent retention.

   Implication

   - The variety of development tools, programming languages, supporting systems (middleware, data and records management, platforms, etc.) must be minimized or standardized on the smallest number of alternatives.

Ground rules and Practices

These provide the preparatory tasks and ongoing practices to be observed and followed by agency systems developers for overall best results and adherence to this enterprise architecture:

1. **Common vision:** An agency's business and IT staff must have a common vision of both its business functions and the role of technology in those business functions. They jointly have the responsibility for defining IT needs and ensuring that the systems delivered by the development teams provide the projected benefits.

   Justification

   - Executive leadership of an agency is responsible for its mission. Information technology staff provides automation of processes to aid in accomplishing that mission. Business and IT purposes must be synchronized to best accomplish the mission.

2. **Business processes drive technical architecture:** The technical architecture of any individual system must be driven by the business processes of the enterprise.

   Justification

   - There must not be a deployment of technology for technology's sake. Effective deployments are focused on the mission and goals of the enterprise.

3. **Reengineer first:** New information systems will only be implemented after business processes have been analyzed, simplified, or otherwise redesigned.

   Justification

   - Avoids automation of flawed processes. Work processes will be more streamlined, efficient, and cost effective. Automation of those processes will be easier to implement and maintain.

4. **Design for sharing:** Identify opportunities for cross-functional components or subsystems and implement them in such a way that there is an opportunity for reuse by any other agency or layer of the government.

   Justification

   - Sharable components must be built as sharable from the beginning. It is difficult and expensive to do so after the fact.

5. **Design for growth:** Err on the side of infrastructure over capacity rather than under capacity. Fixed investments should be oriented toward purchasing the most capacity or capability available within organizational financial limitations. This can create the lowest total cost of ownership while creating the greatest flexibility for future growth.

   Justification

   - Growth in demand of IT support systems has historically been greater than envisioned. Building extra capacity up front, though it involves larger initial cost, will save in the long run because of there is less need to devote technical and management talent to upgrade projects on a more frequent basis.

6. **Design for performance and reliability metering:** Applications and technology components (processors, network, etc.) should be implemented in such a manner that performance measurement and quality assurance data may be captured to support management and analysis of the IT environment.

   Justification

   - The most effective use of systems can only occur if it is known when they are approaching limits. Forecasts for upgrades for capacity or to cure reliability issues can only come from statistical measurements.

7. **Tiered and Partitioned design:** The logical design of components, subsystems, application systems and databases should be clearly partitioned. These partitions must have well-defined interfaces established.

   Justification

   - A change in a database or business rules can affect many large programs, if they are not partitioned. Logical boundaries are needed to separate components from each other. Modular design is more adaptive to changes in internal logic, platforms, and structures. It is the interfaces that allow partitioned components to interact well.

8. **Use industry standards:** Priority should be given to products adhering to industry standards and open architecture.

   Justification

   - Provides ability to leverage the knowledge and efforts of others. Risk is reduced. Proven solutions are implemented.

9. **Set realistic expectations:** Set the right results expectations among development staff and users/customers regarding quality, cost, and delivery time of new systems. Recognizing that tradeoffs in these three attributes are critical to realistically meeting the requirements.

   Justification

   - A new system with high availability and performance cannot be implemented if lowest cost is a driving criteria. Tradeoffs in reliability or performance against cost must be made on a case-by-case basis in the best interest of the business purpose**.**

Domain Architectures

This table contains a listing of the individual Domain Architectures and the chapter groupings where they may be found:

Domain	Chapter
Network	Chapter 2
Platform and Storage	Chapter 3
Data and Records Management	Chapter 4
Data Interchange	Chapter 5
Application	Chapter 6
Middleware	Chapter 7
Presentation and Accessibility	Chapter 8
Collaboration and Workflow Tools	Chapter 9
Security	Chapter 10
System Management and Reliability	Chapter 11

2. Network Architecture

Purpose

Network architecture describes a common, high-performance, reliable, broadband network infrastructure providing data, video and voice communications for the State's distributed information processing and publishing environment.

Scope

This chapter defines network infrastructure technologies and practices in the following areas:

Physical WAN
Transport (data, video, voice, Internet)
Inter-agency access
DNS service and domain name assignment
Firewall infrastructure (see also the Security Architecture section)
Remote access
Private connections
IP address assignment
Electronic messaging infrastructure
LAN practices for converged-capable networks

The Hierarchy of the State Internet:

Like most large-scale data networks systems, the State's network is actually an internet; that is, a network of networks. Each agency or other State division has a single or set of Local Area Networks (LAN) or, if it has multiple sites, one or more Wide Area Networks (WAN) that are interconnected to larger external networks through devices. An agency network could be considered an enterprise network for that agency or division of government. That enterprise network is then connected to the State enterprise inter-agency network through one or more border devices.

It is the scope of this domain architecture to describe the principles and standards to be used in constructing and operating that inter-agency network. This network is currently under the administration of a single service organization (Office of Enterprise Technology (OET)) and provided as a common resource to all agencies and divisions of State government. This network system provides a variety of resources and services in common to all agencies including IP address management, domain name management, electronic mail routing and security services. It is this facility that provides the underlying platform upon which multiple inter-agency applications and data sharing can occur.

Though the scope of these standards are focused on the inter-agency network, it is in the best interests of the enterprise as a whole if all agencies and divisions of government employed these principles, practices, standards and guidelines to their internal enterprise network designs also. This will provide a consistent high-performance and secure State internet that can best realize the benefits of sharing and interoperability.

Principles

1. **Integrated WAN:** A single integrated wide area network (WAN) with a reliable high-bandwidth Internet connection, centrally designed, deployed, managed, and maintained, is the backbone of an enterprise architecture and is necessary to support a variety of communication requirements including, data, image, voice, and video.

Rationale

- It allows access to a wide spectrum of information, application and system resources regardless of location or business unit. Access to resources can be obtained in a timely manner by requesters when and where needed throughout the enterprise.
- It expands the scope of an organization domain by allowing them to reach out to customers and suppliers through access to the Internet and through the provision of remote access services.
- It acts as the delivery mechanism for the distributed computing services required by a dynamic business.

Implication

- Any product or application not designed for a networked environment is limited in the long-term.
- The network must be capable of being the delivery mechanism for distributed services in an N-Tier architecture.
- All inter-agency WAN networks must be centrally designed and maintained by OET. All external devices must be centrally managed by OET or otherwise carefully cataloged and controlled.

2. **Availability and performance:** The availability of the network all day and every day, and its ability to adequately carry the required loads must be a high priority in all deployment plans. Networks must be designed and built with the safety and security of data being a high priority. User access should be a function of authentication and authorization, not of location.

Rationale

- Networks now serve a critical and indispensable role in the enabling of execution of business functions and processes and access to the State's information.
- The State's information must be equally protected and safeguarded in transit as well as in storage and processing.
- Users (State staff and partners) need to access services from multiple sites within the enterprise, from a variety of public and private networks, and from the Internet.
- Clients (general public and other organizations) need to access services from a wide-ranging set of external points that vary over time and place.
- Procedures must be carefully prepared to counter or contain security threats that may impair availability.

Implication

- Reliable networks attempt to contain no single point of failure. Networks are comprised of many components, and are only as reliable as the weakest link. Reliability must be built-in, not added-on.
- Bandwidth must be sufficient to accommodate new and expanding applications, different types of data (e.g., voice, data, image, and video), and a variety of concurrent users.
- The network must be designed to minimize latency. Data must pass across the network in a timely manner so that business decisions can be based on up-to-date information.

- Network must be monitored to track relevant parameters

3. **Standard protocols:** A statewide network must be based on industry-proven, open, vendor-neutral protocols as defined by accepted industry, governmental and Internet standards organizations such as the IETF, ICANN, IEEE, ANSI, ITU, W3C, Frame Relay Forum, DSL Forum, CableLabs, and others similarly recognized.

   Rationale

   - Supports flexibility and rapid adaptation by allowing the state to choose from a variety of sources to select the most effective network solution.
   - Keeps the state enterprise in step with and easily interoperable with external organizations' networks.

   Implication

   - No further deployments of non-standard or other proprietary protocols at the physical, data link, network or transport levels.

4. **Remote access documentation:** Reliability and security of the State's Wide Area Network will require complete documentation within each agency of existing links and tight control of expansion of additional links

   Rationale

   - Required as a first step to best contain and manage the risk of unauthorized access, denial of service, intrusion and vandalism on State assets.
   - The catalog will illustrate which connections are at risk for intrusion and need immediate attention.

   Implication

   - All existing links not compliant with these principles must be carefully documented, cataloged and audited for level of security.

5. **Remote access central management:** The ultimate reliability and security of the state's Wide Area Network will require a securely configured and managed set of external devices, whether low or high bandwidth.

   Rationale

   - A proliferation of "back door" access points increases the likelihood of intrusion and damage to State assets beyond the compromised LAN.
   - The ability to quickly and surely respond to intrusion or denial of service attacks is much more difficult if there are an excessive number of uncontrolled access points.
   - Central management per agency provides the economies of scale that allows the best solution in the most cost-effective manner.

   Implication

   - Remote access for off-campus state employees, business partners, or the general public must be done through a common per agency system.

Best Practices

1. **Reliability:** All WAN network segments of a critical nature should have redundant ports and redundant diversely routed links with automatic rollover. InterTech should maintain hot spares to

replace core network components and an inventory of cold spares to cover all agency device and internal routing and switching equipment.

Justification

It can often take considerable time to diagnose a failure. With the need for availability to state workers, policymakers and citizens, critical systems must not be unavailable..

2. **Capacity planning:** Capacity surges of +15% should be engineered into all LAN and WAN segments. WAN link upgrades should be implemented when sustained load is at an average 65% of capacity.

Justification

Proper performance of IP requires minimal congestion on any link. Lead times for WAN lines from telecomm vendors can be lengthy for large-capacity lines. It is necessary to start the upgrade process early enough to prevent overload.

3. **Data movement:** Deploy heavily used data sources topologically close to the applications using them. Perform large batch updates or data movement in non-prime hours.

Justification

It is much more cost-effective in equipment capacity and line charges to deploy short-distance high-bandwidth data trunks for large-volume data movement.

Technologies, Components and Methods

Category	Transitional	Current	Emerging	Responsibility and References
Physical layer	Cat 3 UTP Coax	**Cat 5, Cat 5E UTP** **Fiber** Cat 6 IEEE 802.11b	Cat 7 IEEE 802.11a IEEE802.11g	Bluetooth Omitted from this list until security issues are addressed
Data link layer	Token ring Ethernet 10Base2 Ethernet 10BaseT Wireless CDPD ATM	Ethernet 100BaseT Ethernet 1000BaseT Frame relay Fiber channel	Ethernet 10000BaseT Packet over SONET MMDS, LMDS, microwave	
Network and Transport	SNA IPX	**TCP & UDP on IPv4**	TCP on IPv6	

Traffic engineering	ATM	MPLS QOS		
LAN interconnect	Hubs	SNMP managed switches		
Addressing & naming		**Domain Name System (DNS).** **All state names must be accessible from the state.mn.us domain. (for example, mail and web addresses using state.mn.us names work) but agencies may use other domains as well.**	IPv6 address assignment rules to be determined.	
Remote access physical layer	V.32 V.34	V.90 PPP ISDN BRI, PRI DSL Cable modem	MMDS LMDS High bandwidth SDSL VDSL	
Remote access protocol layer	SLIP	SSL / VPN		
Interior gateway protocol	RIP	OSPF MPLS suite		
Exterior gateway protocol		**BGP4**		
Video/Data conferencing	ITU H.320 **MPEG**	**H.323v2** **T.120**	H.323v4 H.239 MPEG4	
Video streaming			RTSP MPEG4	

Remote management	Proprietary	SNMP version 1, 2 MIB (RFC 1398) MIB II		
Voice	Centrex	PBX VoIP IP telephony VoIP with SIP		
Mail gate-ways and servers		**Central filtering gateway with dis-tributed agency servers.**		
Domain name servers		**Single statewide primary and sec-ondary, topologi-cally and geo-graphically diverse.**		

Table Formatting:

Plain text: Guidelines — strongly recommended for interoperability and full compliance.

Bold underline: Standards — mandatory for compliance.

Definitions:

Transitional: those that are twilight, retired, or soon to be retired technologies, components and methods and should be discouraged from new implementations. This is not to imply that existing systems need be retired or replaced immediately, but that the use of these products and services should not be extended in any future planning and development.

Current: those that are preferred or required and should be used when making design and implementation decisions.

Emerging: those that include near-term directions and options that need continued monitoring to find applicability within the State IT infrastructure. Included are technologies that are not yet fully production-worthy but are potential candidates for prototype implementations. Continued market acceptance and adaptation will likely move these solutions toward the growth phase of the lifecycle, and inclusion in the statewide architecture will become apparent.

Responsibility and References: what party or group is responsible for keeping this item updated as business needs or technology and industry trends evolve, and/or, a URL or other reference to a defining document or standards document that specifies detail for the technology, component or method.

3. Platform and Storage Architecture

Purpose

Platform and Storage Architecture identifies technology hardware platforms and the related operating systems to support the State of Minnesota's current and future business system requirements. As the State moves to a more enterprise-wide perspective, Adherence to standards will reduce the total cost of ownership and increase interoperability. The Platform Domain will assist the platform decision-making process and promote data integration among agencies. It will ensure easier integration by using compatible technologies.

Scope

This domain includes end users' platforms as well as the applications and database platforms. The architecture is composed of the following technology components:
High-end, mid-range, economy server standard
Workstation capabilities
Storage Area Networks
Mirroring and backup practices
Mail servers
Web servers

Principles

1. **Interoperability of platforms:** Platforms must be designed, acquired, developed, or enhanced such that data and processes can be shared and integrated across the enterprise and with Minnesota's business partners.

   Rationale

   - Increase efficiency while better serving customers (e.g., the public, agencies, etc.).
   - Ensures more accurate information, with a more familiar look and feel.
   - Integration leads to better decision making and accountability.

   Implication

   Impact on an enterprise-wide scale is required when acquiring platforms.

2. **Consolidated storage:** Storage implemented as a separate component in configurations of multiple or clustered subsystems capable of concurrent access is the best strategy for reliability and scalability.

   Rationale

   - Eliminates the need to upgrade servers when more storage is needed.
   - Improves the flexibility of moving storage among servers to balance need and availability.
   - Reduces down time and disruption to add storage to servers.

- Achieves economies of scale with larger storage units that can be partitioned among servers as needed.

Implication

- Requires increased knowledge of application storage needs so that meaningful capacity planning can be done.
- Requires expertise in storage architectures and configurations such as Redundant Array of Inexpensive/Independent Disks (RAID), Network Attached Storage (NAS), and SAN Storage Area Network (SAN) systems and the ability to use them well.
- Must add an additional software layer to the operating system to provide support (such as virtualization) for RAID and SAN that are not part of its native capability.
- Requires additional software for storage management including backup and recovery.
- Requires additional knowledge and skills for file protocols such as Network File System (NFS) and Common Internet File System (CIFS) for use with NAS.

3. **Minimization of platform configurations:** Interoperability is better supported with a small number of consistent configurations for deployment across the enterprise.

Rationale

- Reducing uniqueness in product selection and standardization reduces support, maintenance costs, and simplifies training and skills transfer.
- This is the most efficient approach to enterprise-wide infrastructure configuration and maintenance.
- By constantly 'tweaking' the performance of an individual server or desktop computer rather than replacing them, a multitude of unique configurations is maintained, thus increasing support and maintenance costs.

Implication

- Deploy applications on uniformly configured servers ("If in doubt, use the bigger box").
- Plan to replace multiple, non-standard, configurations with a small number of consistent configurations.
- Plan for the regular replacement of platform components to ensure the retirement of obsolete and unique configurations.
- Limits product choice and vendor selection when developing new applications.

4. **Industry Standards:** Priority will be given to products adhering to industry standards and open architecture. Currently, open and industry standards may conflict and care must be taken to remain flexible and avoid being locked into proprietary solutions during this period of rapid change in the IT field.

Rationale

- Avoids dependence on individual vendors.
- Reduces risks.
- Enables greater use of commercial-off-the-shelf solutions.
- Allows flexibility and adaptability in product replacement.

Implication

- Requires a culture shift.
- Need to establish criteria to identify standards and the products using them.

- IT organizations will need to determine how they will transition to this mode.
- Migration planning to move to industry-standard well-supported platforms must be emphasized..

5. **Scalability:** The underlying platform and storage infrastructure a must be scalable in size, capacity, and functionality to meet changing business and technical requirements.

   Rationale

   - Reduces total cost of ownership by reducing the amount of application and platform replacements needed to respond to increasing or decreasing demand on the system.
   - Encourages reuse.
   - Leverages the continuing decline in hardware costs.

   Implication

   - Scalability must be reviewed for both “upward” and “downward” capability.
   - May increase initial costs of development and deployment.
   - Will reduce some solution choices.

6. **Platform Security and Integrity:** Platform architecture enhances system integrity
   - Hardware and Software should provide a separate memory space for each operating system, sub-systems, and applications Encourages reuse.
   - Instruction execution should provide hardware encoding (protection) and software interrogation for the read or write of memory.
   - Only one security function, or control point for internal security, and all functions and operations must use it
   - Should have more than one level of operation so that only certain code, functions, or operations can be executed, if authorized to be at that level.
   - Limit “Superusers” authority or minimize and control: Read/Write memory access, System Capabilities (Mount, Start/Stop, Trace, Priority), System Resources (CPU time, Memory size, Processes, Threads, and Memory Map (control blocks)).

   Rationale

   - Improve security, integrity, and operation of the platform.
   - Reduce interruptions of service and provide greater quality.
   - Reduce exposures to hacking or unintentional errors.
   - Improve confidence and reliability of the system.
   - Provide audit trail for changes and violations.

   Implication

   - If we move applications from platform to platform the security and integrity would be understood.
   - Increase knowledge and understanding of exposures and evaluate platform environments.
   - Evaluate the use and implementation of platform security.
   - Evaluate application requirements and security needs to select the appropriate platform as a part of system design, not application implementation.

7. **Performance management:** Platforms and storage systems are best managed by a single performance management product capable of supporting the diverse platforms utilized across the enterprise.

   Rationale

   - Provides a common look of enterprise resource usage and performance for operations, support and management across the enterprise.
   - Reduced installation, support, training, skills transfer and maintenance costs of the performance management product
   - Capability to gather performance data in a central "database." The consolidated performance data can be used to build models of current workloads for capacity planning and forecasts of future resource requirements.

   Implication

   - Requires cooperative efforts across agencies to select the best system and coordinate installation(s) and operational practices.

Best Practices

1. **Uniformity of platforms:** Major applications should be placed on uniformly configured servers. New major applications should be written for the Enterprise Technical Architecture recommended platforms.

   Justification

   - Makes overall maintenance, support and recovery less expensive.

2. **Reliable design:** Design mission critical systems without a single point of failure to the largest extent practical. Distributed systems can be designed to be robust. Small granular servers make it easier to replicate services for increased availability. Systems should be designed to permit continued operations, albeit at reduced throughput, when a server fails in normal operations or in the event of a disaster.

   Justification

   - Supports Conceptual Principle of integrated reliability.

3. **Upgrading:** Design servers to be field upgradeable. Rapid changes in business processes are enabled in part by implementing a platform technical infrastructure that exceeds the immediate application requirements. This means that agencies should purchase servers with upgradeable components so they are able to be expanded more easily and cost effectively.

   Justification

   - Field upgradeable servers provide maximum flexibility and adaptability for growth and new functionality.

4. **Administration policies:** Adapt structured administration policies and procedures to the administration of server platforms of all sizes.

   Justification

   - All servers require a level of attention based on service and importance rather than physical size and capacity.

5. **Disaster recovery:** Disaster recovery plans and technology should be consistent between various technology types (Mainframe, UNIX, NOS).

   Justification

   - Services are distributed among a variety of systems and require equivalent recovery emphasis.

6. **Storage Refresh:** Refresh physical storage media periodically to compensate for media degradation.

   Justification

   - A wide range of efforts and practices must be employed to ensure the safety and reliability of the State's most important assets.

7. **Single host, single service:** Avoid installing multiple services on a single host. Each individual key service should have its own host.

   Justification

   - Key services should be isolated on separate hosts so as not to affect each other if one should crash or need intervention. Multiple services can go off line when there is a fault in only one.

Technologies, Components and Methods

Category	Transitional	Current	Emerging	Responsibility and References
Workstations (desktop or portable)	3270	Able to execute applications or create documents according to specifications described in Collaboration and Workflow Architecture		Collaboration and Workflow Architecture
Servers	VAX/VMS Windows NT	Windows 2000 POSIX compliant Unix, OS400, Netware 5.x, OS/390, Unisys HMP	Linux Windows XP Windows 2000 Data Center Edition Netware 6.x	
DataBase Management System	Supra	JDBC or ODBC compliant		
Thin Client/Terminal	3270 VTxxx 3270 Emulation	Citrix/Winframe	Java VM	
Mail Servers		SMTP, POP, IMAP compliant		
Storage Area Networks (SAN)				[Waiting for industry standards]

Table Formatting:

Plain text: Guidelines — strongly recommended for interoperability and full compliance.

Bold underline: Standards — mandatory for compliance.

Definitions:

Transitional: those that are twilight, retired, or soon to be retired technologies, components and methods and should be discouraged from new implementations. This is not to imply that existing

systems need be retired or replaced immediately, but that the use of these products and services should not be extended in any future planning and development.

Current: those that are preferred or required and should be used when making design and implementation decisions.

Emerging: those that include near-term directions and options that need continued monitoring to find applicability within the State IT infrastructure. Included are technologies that are not yet fully production-worthy but are potential candidates for prototype implementations. Continued market acceptance and adaptation will likely move these solutions toward the growth phase of the lifecycle, and inclusion in the statewide architecture will become apparent.

Responsibility and References: what party or group is responsible for keeping this item updated as business needs or technology and industry trends evolve, and/or, a URL or other reference to a defining document or standards document that specifies detail for the technology, component or method.

4. Data & Records Management Architecture

Purpose

When Minnesota state agencies conduct activities electronically, they will need to create and maintain accurate electronic records of those activities. Data architecture describes how the State's electronic data should be defined, stored, maintained and retained to facilitate processing, accessing, sharing and analyzing from any part of the enterprise for appropriate constituencies according to existing federal and state laws. Records management describes how the State's electronic information is managed, preserved, and disposed of. The goals of data management and the architecture to support it include decision support for government and other indirect and direct services to citizens of Minnesota and the world.

Data is a representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means.[1] Relative to today's computers and transmission media, data is encoded as representations of symbols or values in binary digital form to which meaning is or might be assigned. Minnesota Statute defines government data as "all data collected, created, received, maintained or disseminated by any state agency, political subdivision, or statewide system regardless of its physical form, storage media or conditions of use.[2]"

A ***record*** is a set of data or information that is treated as a unit and inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form. "Electronic record" means a record created, generated, sent, communicated, received, or stored by electronic means.[3]

Records management is a "program for the application of efficient and economical management methods to the creation, utilization, maintenance, retention, preservation, and disposal of official records.[4]" Records management is the statutory responsibility of every unit of government.

Metadata is the term used to describe the structured description of information resources required to make that data understandable, usable and sharable.

Scope

This architecture provides for the construction, management and use of high-quality, consistent data for online transactional processing and online analytical processing, executive information systems, decision support systems and standard reporting systems. The architecture is composed of the following technology components:

Data Definition – creation, naming standards
Data Storage – database design, disaster recovery

[1] Federal Standard 1037C, Glossary of Telecommunication Terms, 1996 (http://www.its.bldrdoc.gov/fs-1037/)
[2] Minnesota Statute section 13.01
[3] Minnesota Statute section 325L.02
[4] Minnesota Statute section 138.17

Data Access – privacy, security, legal classification, access methods
Data Maintenance – stewardship, backup, recovery
Data/Records Retention – records management, preservation

Metadata is applicable to all of the above technology components

The domain scope does not include document management (covered in Chapter 9, "Collaboration and Workflow Tools Architecture").

The domain scope does not include information architecture. Though a comprehensive information architecture would be a logical step prior to constructing this data architecture, this was not available. Therefore, the scope of this domain was expanded to include some aspects of information architecture in its coverage of metadata standards. The establishment of a more comprehensive information architecture would greatly improve the ability of state systems to share and operate cooperatively. Such an effort would be larger and more extensive and should subsequently be initiated as part of an effort to complete all the levels of architecture necessary to provide the best long-term results.

Principles

1. **Data is a State Asset:** Data is valued as a state enterprise asset, managed by specified custodians on behalf of the citizens of Minnesota, and used to enhance and accelerate decision-making subject to the laws, regulations and policies governing data security and privacy. Data in Minnesota state government information systems must be freely sharable within the limits of explicit security and privacy laws.

   Rationale

   - Enhance and accelerate business decision-making that requires information beyond the traditional borders of a system or agency.
   - Facilitate new enterprise-wide or multi-agency solutions.
   - Expand knowledge of data existence so that its value can be recognized and used.
   - Enable public access.
   - Secure data as appropriate to their classification.

   Implications

   - Information systems must be designed to accommodate decision-making and authorized data sharing beyond the borders of an agency to address the larger communities of interest.
   - A policy pertaining to data stewardship must be developed. Stewardship must be identified or assigned.
   - Data and its value must be identified by its current keepers. It must be authenticated, documented, and managed appropriately.

2. **Data Quality:** Information of appropriate quality is essential to making good decisions**.** Information systems should be designed to collect and maintain data of appropriate quality. Minnesota Statutes, Section 13.05, subdivision 5, requires that data on individuals be accurate, complete and current. Quality depends on the "user," as what is quality data to one user for a given purpose may be inadequate to another for a different purpose. Quality data meets the user's needs.

   Rationale:

   - The utility of a data resource depends on its quality.
   - The quality of the data must be known in order to weigh it properly during decision making.

   Implications

   - Information system designers must consider other possible uses and users of the data when determining what to collect and how to maintain it.
   - Documentation of the data should include a description of the data quality and its appropriate usage. This includes the quality of the specification of the data and the correctness of the data values.
   - End users should have read-only access to data warehouse data.
   - Editing and validation rules in source systems should be saved for operational and historical purposes. The retention period for these data rules should parallel the time period on the approved retention schedule for the records containing the data.
   - Data scrubbing rules for data warehouses should be saved for operational and historical purposes. The retention period for these data-scrubbing rules should parallel the time period on the approved retention period for the records containing the data.

3. **Data Practices:** Systems must be designed and built to meet and operate within the legal requirements of federal and state laws. The primary state law is the Minnesota Government Data Practices Act <http://www.revisor.leg.state.mn.us/stats/13/>. (See also Chapter 5, "Data Interchange Architecture," Chapter 6, "Application Architecture," Chapter 9, "Collaboration and Workflow Tools Architecture," and Chapter 10, "Security Architecture.")

   Rationale

   - Facilitate access to data as permitted and required by law.
   - Restrict access to data as required by law.
   - Facilitate data sharing as permitted by law.
   - Prevent data sharing as required by law.
   - Provide rights for individuals who are the subjects of data.

   Implications

   - Each agency is responsible for knowing and following the federal and state laws that apply to the data they maintain and for designing automation systems accordingly.
   - The provision of rightful access to data balanced with the protection of data from unauthorized access must be conscientiously and continually evaluated and applied.
   - The electronic storage of data must incorporate a tracking method of data classification and considerations that are known for any particular data element, record, or dataset.
   - The process of releasing data must include steps that check against the most current data classifications and considerations, such as the Tennessen Warning Notice and the Federal Privacy Act, and resolve conflicting mandates expeditiously.

- Systems that are designed without meeting the proper requirements will subject an agency to expense, embarrassment and litigation.
- State agencies have the following responsibilities regarding government data:
  (1) to provide authorized access;
  (2) to prevent unauthorized access; and
  (3) to prevent the unauthorized sharing of data.
  (4) to assure that individuals can effectively exercise their rights under the Minnesota Government Data Practices Act.

4. **Metadata:** Common deployment of data documentation schemes promotes data reusability, reliability, and the possibility of sharing across the enterprise.

   Rationale

   - Metadata facilitates a number of activities such as data/record location, retrieval, evaluation, management, use, and disposition.
   - Standardized metadata schemes allow data element definitions of like metadata to be shared and help to build common data models.
   - Data documentation allows data to be used consistently across applications.
   - Controlled vocabularies or thesauri allow consistency and interoperability across metadata sets.

   Implications

   - Use standardized procedures to thoroughly document information resources.
   - When designing or modifying a system that employs metadata, review the standardized scheme to ensure consistency with metadata and data element definitions.
   - Where appropriate, employ and publish controlled vocabulary from thesauri, standards, or other controlled lists for populating specific metadata elements.
   - Develop a statewide metadata repository.

5. **Preservation, Backup and Recovery:**. Reliability and long-term availability of State data is paramount. Data must be protected from intentional or unintentional damage.

   Rationale

   - The State's data is its most important asset. Its preservation and safeguarding must be primary design and implementation criteria.
   - Backup and recovery must meet business continuation needs. (See also Chapter 3 "Platform and Storage Architecture" and Chapter 11 "System Management and Reliability Architecture.")

   Implications

   - Appropriate backup and recovery strategies and methods must be designed, tested, and implemented as an integral part of all data storage systems.
   - All backup and recovery strategies must address the business requirements of the data regarding availability, accuracy, and timeliness of data.
   - Backup media should be included on the agency's records retention schedules, with retention periods long enough to support recovery operations but no longer than that of the official records.
   - Disaster Recovery/Business Continuity plans must be developed, tested, revised, and implemented when required for data that is critical to business operations.
   - Data must be periodically tested for recoverability according to requirements for its use and preservation.

- Database schemas, structures and data definitions need to be backed up along with the data.

6. **Data Definition:** Sharing data among organizations and systems is best accomplished when the data is uniquely and accurately identified. Data meaning and clarity are enforced through data element definitions that consist of a written description of what the element is and how it is used, its domain values, and its physical format (length, type, storage format). Data element names are structured with consistent format and content.

Rationale

- Accurate identification ensures that data can be defined in one place, then shared with or transmitted to another place without losing its meaning or clarity.
- Data definitions allow for maximizing the value of data resources (and resource investment), sharing data with others, and meeting customer data needs.
- Properly created data definitions help manage data resources by ensuring integrity (without duplication), providing clarity of meaning, and making data accessible to those who need it through precise identification of the required data.
- A good data element definition strategy with proper discipline and management helps with data consolidation by providing a common point of continuity. Good data names also help reduce data costs (especially those associated with data redundancy) and improve the quality of data and other information resources.

Implications

- Policies, standards, and methods for data administration should be developed at an enterprise level defining the:

  Policies for how statewide data is administered; who can name or define data and data model components or approve data definitions and data-name structure, format and content; how do data names and definitions get implemented or cross-referenced to existing data; and the criteria and methods for maintaining, modifying and adding to the rules and policies.

  Rules for the use of (synonyms, homonyms, aliases) for the enterprise's data.

  Rules for when standard names and definitions must be used for computerized data and data model. These rules should focus on the following classes of data:

  - Data that will be shared: data that is received from others, provided to others, or for which there are other stakeholders (such as local government or private sector collaboration).

  - Data involved in inter- or intra-agency efforts: community data, created or used by multiple organizations, or departments within a larger organization.

  - Data that must be accessible to the public.

  - Data for current systems development or integration projects: to realize internal data integrity improvements for projects currently underway (especially those that will have to create data names or match / cross-reference duplicate data).

- Data involved in current modeling efforts: standards should be developed for the naming and definition of entities, relationships and attributes on object and data models. Without good standards on models, it will be difficult to integrate models or share data.

- A mechanism should be established for deciding how communities of interest will agree on standard data definitions within their purview.
- Standard definitions should be developed for qualifying enterprise data.

7. **Records Management:** Accurate and well-kept records, including those in electronic form, are critical to the State's ability to provide its services, present evidence, provide historical documentation, preserve its heritage, and allow its actions to be reviewed and audited. These records must be created, preserved, retained and disposed of as required by law.

   Rationale

   - Records management is concerned with the systematic analysis and control of recorded information in all formats including paper, photographic, and electronic. Records have a distinct legal and administrative status. This may not be true of all information and documents in an information system. Records must be managed as important resources with special requirements that may be distinct from other information resources.
   - Electronic records management principles are relevant whenever computer systems are used to process information and to provide trustworthy evidence of activities and transactions.
   - All government electronic records fall under the mandates of the Official Records Act[5] and the Records Management Act.[6]

   Implications

   - Agencies must understand how the legal mandates for managing their records apply to all existing and any new processing and storage technologies they employ.
   - Recordkeeping requirements must be clearly identified when new systems are designed or when existing systems are upgraded.
   - The official copy of a record must be retained for at least as long as the retention period specified in the agency's records retention schedule. Convenience copies of records may be discarded at any time and should not be kept past the end of the retention period of the official copy.
   - The Official Records Act requires that responsible authorities make and preserve all records necessary to a full and accurate knowledge of their agency's official activities. The act acknowledges that government records may be in the form of computerized records and shall be made on a physical medium of a quality to insure permanent records. The chief administrative officer of each agency is responsible for the preservation and care of the agency's government records.
   - The Records Management Act requires each agency to manage its records effectively and economically. No agency can dispose of its records without authorization from the records disposition panel.

Best Practices

-

[5] Minnesota Statute section 15.17
[6] Minnesota Statute section 138.17

1. **Replicated data:** Design for all replicated data to be read-only.

   Justification

   - Updates should occur through the source where the data originates to facilitate the ease of data management.
   -

2. **Data practices and recordkeeping design consideration:** Include data and records capture, identification, management, retention scheduling, and data practices requirements in the business rules of systems. They should be addressed in the system planning and development stage rather than waiting until the end of the records lifecycle.

   Justification

   - Accurate data and recordkeeping are prime directives for state activities and must be designed into the system as part of its core functions, not as an adjunct activity.
   - The legal mandates of data practices and recordkeeping demand specific functionalities be designed within systems to create trustworthy systems.

3. **Database design and data storage:** Databases and data storage should be designed to meet the processing and security requirements for which the data is being collected and used. Also, consider database scalability implications in the database design.

   a) When OLAP (On Line Analytical Processing) requests will adversely impact the performance of an OLTP (On Line Transaction Processing) application, separate database designs and data storage should be used.

   Justification

   - In order to optimize either type of database for performance, separate database designs may be required. Data structures, such as star or snowflake schemas, multidimensional databases, and flat files are better suited for OLAP applications.

   b) With OLTP applications, where high performance, availability, and reliability are critical for an application, modular design for the database and data should be used. Techniques to accomplish this include: spreading multiple databases across servers, designing databases to be split by functions or subject areas, and partitioning table data physically across storage devices.

   Justification

   - Parallelism permits requests to be broken down and processed simultaneously rather than serially.
   - Scalability allows for future growth and demand.

   c) Data warehouses should be implemented as ODBC/JDBC compliant databases for OLAP, Executive Information Systems (EIS), Decision Support Systems(DSS) and read-only queries and reporting.

   Justification

   - New legislation is constantly redefining the services provided by the State. An accelerated decision-making process is required, using timely, easily accessible, understandable, reliable, and high-quality information. When a data warehouse is properly implemented using an ODBC/JDBC compliant database, authorized end users can perform their own ad hoc queries and reports against the data warehouse relieving application programmers from developing as many reporting programs.

d) It can be advantageous to keep atomic- as well as summary-level data in data warehouses. Atomic-level data is transaction-level data that can be replicated in a read-only data warehouse. This data can address the business need to recast history.

Justification

- Due to the fast pace of business change, many organizations are going through multiple reorganizations. When these occur, many decision makers want to recast history (e.g., to get a feel for what test scores would have been like if the number of school districts were already reduced to respond to legislation or funding). If only summary-level historical data is kept in the data warehouse, it is not possible to recast history.

e) Data extraction and transformation rules for data in OLAP, EIS, DSS and other types of data warehouses need to be documented in a data warehouse repository and/or metadata repository.

Justification

- Data extraction and transformation are important aspects of a data warehouse in terms of data integrity. These provide the information map connecting the data populating a data warehouse with its sources.

f) Consider the network when designing database systems. The impact of the volume of data moving across the network and required latencies must be taken into account when designing databases and information systems.

Justification

- The network is a partner to an application and can impact performance and design. Estimates of the impact on the network when partitioning and placing data must be done.

g) The security requirement for data are dependent on the classification of the data maintained by an agency. Appropriate security for the data must be provided in:

- the database design and implementation
- the system design and implementation
- the storage of data
- the network used to transfer data.

Justification

- The Minnesota Government Data Practices Act requires that an agency maintain appropriate security safeguards for data on individuals.

4. **Data audits:** Ensure data is sufficiently edited initially before storing electronically and perform periodic validity audits to ensure an on-going high level of confidence in the quality and integrity of the data.

Justification

- Operational systems and decision-making systems require high-quality data. The costs of bad data can include bad decisions, lost opportunities, customer frustration, public embarrassment, loss of revenue, ~~and~~ loss of productivity from repair efforts, and possible negative consequences to individuals.
- It is the responsibility of both the business users and the assigned stewards and custodians to ensure the integrity and quality of data.

5. **Metadata standards**: Use identified metadata standards appropriate to specific business functions and data communities.

   Justification

   - Standard metadata facilitates the evaluation of data and records and allows for their economical and effective discovery, evaluation, management, disposition and preservation according to law.

Technologies, Components and Methods[7]

Category	Transitional	Current	Emerging	Responsibility and References
Database access		Structured Query Language (SQL) defined in ANSI S3.135-1992 Database Language SQL as delimited by FIPS PUB 127-3		
Cross-platform data encoding and formatting		eXtensible Markup Language (XML)		W3C http://www.w3.org/XML/
		EDI standards as defined by ANSI X.12 HL7		
Application Program Interfaces (API)		Java Database Connectivity (JDBC)		
		Open Database Connectivity (ODBC) Document Object Model (DOM)		
		Simple API for XML (SAX)		

[7] See end of table for column definitions and formatting information.

Category	Transitional	Current	Emerging	Responsibility and References
			Open Document Manage-ment Asso-ciation API (ODMA)	
Geospatial Data: For-mats		Arc/Info coverages		
		Shapefiles (shp)		
		Intergraph .dgn files		
		Arc/Info GRID files		
		ERDAS Image files		
		GeoTIFF		
		EPPL7 raster files		
		EPPL7 .dgt files		
		AutoCAD .dxf files		
		LizardTech MrSID		
		ERMapper ECW		
			Geography Markup Language (GML)	Open GIS Con-sortium (OGC) http://www.openg is.org/docs/02-023r4.pdf
			JPEG2000	Joint Photo-graphic Experts Group http://www.jpeg.o rg/jpeg2000/
Geospatial Data: Accu-racy		**IRM Standard 19, Version 1: A Meth-odology for Meas-uring and Report-ing Positional Accuracy in Spatial Data**		MN Office of En-terprise Technol-ogy

Category	Transitional	Current	Emerging	Responsibility and References
Geospatial Data: Naming		Water Basin Numeric Identifier standard		
		Codes for the Identification of Minnesota Cities, Townships & Unorganized Territories (CTU)		MN Governor's Council on Geographic Information http://www.gis.state.mn.us./committee/stand/ctu_stand.htm
			Hydrographic Data Content standard (in process)	Federal Geographic Data Committee http://www.fgdc.gov/standards/status/sub5_5.html
Geospatial Data: Other			OpenGIS implementation specifications	OpenGIS Consortium http://www.opengis.org/
Multimedia		Moving Picture Experts Group (MPEG-1, MPEG-2 and MPEG-4)		
		Musical Instrument Digital Interface (MIDI)		
			Advanced Authoring Format (AAF)	
			Advanced Streaming Format (ASF)	
			MPEG Audio Layer 3 (MP3)	

Category	Transitional	Current	Emerging	Responsibility and References
			MPEG 7	
			Synchro-nized Mul-timedia In-tegration Language (SMIL)	
			Virtual Re-ality Model-ing Lan-guage (VRML)	
			Visual XML (VXML)	
Character encoding	Extended Bi-nary-Coded Decimal In-terchange Code (EBCDIC)			
		ASCII		
		ISO Latin-1 (ISO-8859-1)		
			Unicode	
File naming and hierarchy		Filesystem Hierar-chy Standard (FHS)		
		Universal Naming Convention (UNC)		
Images: Formats		TIFF		
		PDF		
		SVG		
		PNG		
	GIF			

Category	Transitional	Current	Emerging	Responsibility and References
		JPEG	JPEG2000	Joint Photo-graphic Experts Group http://www.jpeg.org/jpeg2000/
Images: Imaging		**IRM Standard 12, Version 1: Technical Standards for the Reproduction of Government Records Using Imaging Systems**		MN Office of Enterprise Technology
		IRM Standard 13, Version 1: Management Standards for the Reproduction of Government Records Using Imaging Systems		MN Office of Enterprise Technology
Information retrieval		Common Gateway Interface (CGI)		
		Structured Query Language (SQL) defined in ANSI S3.135-1992 Database Language SQL as delimited by FIPS PUB 127-3		
			XML Matching and Structuring language (XMAS)	
			XML Query Language (XQL)	

Category	Transitional	Current	Emerging	Responsibility and References
			Common Indexing Protocol (CIP)	
		Application Service Definition and Protocol Specification (Z39.50)		
	Global Information Locator Service (GILS) Application Protocol			
	Australian Government Locator Service (AGLS)			
Metadata: Cross-domain information resource descriptions		Dublin Core NISO/ANSI Z39.85 (ISO 15836:2003)		NISO / ANSI http://www.niso.org/standards/resources/Z39-85.pdf
		IRM Standard 21, Version 1: Web Metadata Standard		MN Office of Enterprise Technology
Metadata: Data Elements			ISO/IEC 11179: Information technology – Metadata registires (MDR)	ISO/IEC http://isotc.iso.ch/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards.htm (scroll down until you find all six parts of this standard: 11179-1 through 11179-6)

Category	Transitional	Current	Emerging	Responsibility and References
Metadata: Geospatial data		Minnesota Geographic Metadata Guidelines		http://www.gis.state.mn.us/stds/metadata.htm
		FGDC-STD-001-1998: Content Standard for Digital Geospatial Metadata (version 2.0)		Federal Geographic Data Committee: http://www.fgdc.gov/metadata/contstan.html
			ISO 19115: Geographic Information Metadata	ISO: http://www.fgdc.gov/standards/status/iso_19115.html
			ISO 19139: Geographic Information – Metadata Implementation Schema	ISO: http://metadata.dgiwg.org
Metadata: Recordkeeping		**IRM Standard 20, Version 1.2: Minnesota Recordkeeping Metadata Standard**		MN Office of Enterprise Technology
Data Coding: Value Domain Standards		FIPS Pub 5-2: Codes for the Identification of the States, the District of Columbia and the Outlying Areas of the United States, and Associated Areas		http://www.itl.nist.gov/fipspubs/fip5-2.htm

Category	Transitional	Current	Emerging	Responsibility and References
		IRM Standard 15 Version 1: Numeric Codes for the Identification of Counties in Minnesota		MN Office of Enterprise Technology
		Codes for the Identification of Minnesota Cities, Townships & Unorganized Territories (CTU)		MN Governor's Council on Geographic Information http://www.gis.state.mn.us./committe/stand/ctu_stand.htm
		ISO 3166-1: Codes for the Representation of Names of Countries and Their Subdivisions – Part 1: Country Codes		ISO http://www.iso.ch/iso/en/prodsservices/iso3166ma/05database/index.html
Data Element Naming		IRM Guideline 9, Version 1: Data Administration: A Data Naming Primer		MN Office of Enterprise Technology
		IRM Guideline 10, Version 1: Data Administration: A Data Naming Practitioner's Guide		MN Office of Enterprise Technology

Category	Transitional	Current	Emerging	Responsibility and References
Records Management Strategies		Trustworthy Information Systems Handbook		MN Historical Society, State Archives Department http://www.mnhs.org/preserve/records/tis/tis.html
		Electronic Records Management Guidelines		MN Historical Society, State Archives Department http://www.mnhs.org/electronicrecords
		Preserving and Disposing of Government Records		MN Dept. of Administration, Information Policy and Analysis Division http://www.ipad.state.mn.us/records2.html
		DOD Standard 5015.2: Design Criteria Standard for Electronic Records Management Software Applications		Department of Defense http://jitc.fhu.disa.mil/recmgt/standards.htm

Category	Transitional	Current	Emerging	Responsibility and References
			ISO 15489-1:2001: Information and documentation – Records management – Part 1: General ISO/TR 15489-2:2001: Information and documentation – Records management – Part 2: Guidelines	ISO http://www.iso.ch/iso/en/ISOOnline.openerpage
Resource Identifiers and Links		Domain Name System (DNS)		
		Uniform Resource Locator (URL)		
		Lightweight Directory Access Protocol (LDAP) x.500		
			XML Namespaces	W3C http://www.w3.org/XML/
			Digital Object Identifier (DOI)	
			Directory Services Markup Language (DSML)	
			Common Name Resolution Protocol Handle System	
			XML Pointer Language (XPointer)	

Category	Transitional	Current	Emerging	Responsibility and References
			XML Path Language (XPath)	
			XML Linking Language (XLink)	

Table Formatting:

Plain text: Guidelines — strongly recommended for interoperability and full compliance.

Bold underline: Standards — mandatory for compliance.

Definitions:

Transitional: those that are twilight, retired, or soon-to-be-retired technologies, components and methods and should be discouraged from new implementations. This is not to imply that existing systems need be retired or replaced immediately, but that the use of these products and services should not be extended in any future planning and development.

Current: those that are preferred or required and should be used when making design and implementation decisions.

Emerging: those that include near-term directions and options that need continued monitoring to find applicability within the State IT infrastructure. Included are technologies that are not yet fully production-worthy, but are potential candidates for prototype implementations. Continued market acceptance and adaptation will likely move these solutions toward the growth phase of the lifecycle, and inclusion in the statewide architecture will become apparent.

Responsibility and References: theparty or group responsible for keeping the item updated as business needs or technology and industry trends evolve, and/or, a URL or other reference to a defining document or standards document that specifies detail for the technology, component or method.

5. Data Interchange Architecture

Purpose

Data Interchange Architecture provides specialized support for the interchange of information between State of Minnesota agencies. This architecture is expected to handle data interchange between applications on the same platform and applications on different (heterogeneous) platforms. Through data integration, new applications can access the existing business processes and information. An application integration strategy has the potential to reduce software development and maintenance costs for situations that require connecting multiple heterogeneous applications.

Scope

Document generic data typing and conversion services are supported by specifications for encoding the data (e.g., text, pictures, numeric, special characters) and both the logical and visual structures of electronic documents, including compound documents.

Graphics data interchange services are supported by device-independent descriptions of picture elements for vector-based graphics and descriptions for raster-based graphics.

Specialized data interchange services are supported by specifications that describe data used by specific vertical markets. Markets where such specifications exist include the medical, library, dental, and insurance and oil industries.

Electronic data interchange services are used to create an electronic (paperless) environment for conducting commerce and achieving significant gains in quality, responsiveness, and savings afforded by such an environment. Examples of applications that use electronic commerce services include vendor search and selection; contract award; product data; shipping, forwarding, and receiving; customs; payment information; inventory control; maintenance; tax-related data; and insurance-related data.
Fax services are used to create, examine, transmit and/or receive fax images.

1. *Data translation and mapping.* Translates the different communications and data interchanges between two applications.
2. *Transaction explosion.* If configured properly, an application integration interface can take one client transaction and spawn multiple transactions in remote applications.
3. *Front-ending other applications.* An interface can provide a single front end for integrating multiple application systems.

Principles

1. **Self-defining data structures:** Data structures used for interchange should be self defining. to best assure flexible interoperability

   Rationale

   - Readable throughout the enterprise.
   - Breaks the application and database dependency.
   - Facilitates interpretations.
   - Has a built-in method for data validation.
   - The cost of inter-operation is reduced

   Implication

   - Fixed-field flat-file data interchanges are undesirable.

2. **Fitness for use:** Cross agency data use must be supported by sufficient documentation to allow the receiving party to determine fitness for use for a particular application.

   Rationale:

   - A potential exists to misuse data outside the context for which it was originally intended.

   Implication:

   - Data must have formal agreements for interchange.
   - People that source the data would have a responsibility to establish a narrative descriptive record. e.g. use of the Dublin Core specifications or the Minnesota Geographic Metadata Guidelines.

3. **No change of attributes:** When data is transmitted from site to an external organization,
   a. the state ownership of it does not change.
   b. the security or access authorization constraints do not change.
   c. the privacy restriction do not change.
   It is the responsibility of the receiving agency to follow all security, access and privacy constraints. It is the responsibility of the supplying agency to remind or inform the recipient organization of the data constraints.

   Rationale

   - Data remains a state asset and legal requirements on it do not change in transfer.
   - Protection of privacy or confidentiality are not altered with a change in storage location

   Implication

   - Both source and destination of all State data have the same responsibilities to secure and protect data in transit as they do in storage as covered by the data practices act and requirements of the Data and Records Management Architecture.

4. **Data currency:** The recipient of transferred data has the responsibility to assure the currency of the data it receives by verification with the original source as needed.

   Rationale

   - Incorrect or out-of-date data can have significant adverse effects on individuals or organizations, especially in the case of criminal justice information or health information

Implication:

- Structured, and preferably automated, methods must be set up in advance of data transfer to assure currency and accuracy.

Best Practices

1. **XML:** Use XML to automate frequently used business transactions.

   Justification

   - XML is appropriate for agency-to-agency commercial transactions as well as for commerce with outside organizations. Agency-to-agency transactions should exchange mapped data, without requiring the trading partners to go through the generation/interpretation process. The XML schema or DTD should be a W3C standard.
   - The state may require XML capability, and encryption when necessary, of vendors.

2. **Industry Standards:** Use industry standards for transactions that are being performed electronically.

   Justification

   - Be aware that standards will evolve over time, and all participating trading partners will need to synchronize when a newer version is implemented.

3. **Security and Privacy Compliance:** The source and receiving agencies in a data transfer are responsible for complying with the security and privacy requirements of state and federal laws.

   Justification:

   - It is the responsibility of all state agencies to assure compliance with data practices laws and other applicable state and federal laws.

- Technologies, Components and Methods

Category	Transitional	Current	Emerging	Responsibility and References
Cross-platform data encoding and formatting	EDI standards as defined by ANSI X.12 HL7	eXtensible Markup Language (XML)		W3C XML Recommendations:http://www.w3.org/TR/REC-xml ISO/TS 20625:2002, Electronic Data Interchange…XML: http://www.iso.org
Character encoding	Extended Binary-Coded Decimal Interchange Code (EBCDIC)	ASCII ISO Latin-1 (ISO-8859-1)	Unicode	

Category	Transitional	Current	Emerging	Responsibility and References
Images *Long term value* *Short term value - as appropriate*		IRM Standard 12 TIFF GIF JPEG		Images : IRM Standard 12: For Geographically referenced Images see Geospatial Data below.
Multimedia		Moving Picture Experts Group (MPEG-1, MPEG-2 and MPEG-4) Musical Instrument Digital Interface (MIDI)	Advanced Authoring Format (AAF) Advanced Streaming Format (ASF) MPEG Audio Layer 3 (MP3) MPEG 7 Synchronized Multimedia Integration Language (SMIL) Virtual Reality Modeling Language (VRML) Visual XML (VXML)	

Category	Transitional	Current	Emerging	Responsibility and References
Secure transfer	Secure Hypertext Transfer Protocol (SHTTP)	SSH Protocols and Secure Shell Secure Sockets Layer (SSL)	Encryption using KEA and SKIPJACK IP Security (IPsec) KeyNote Trust-Management System Version 2 RSVP Operation Over IP Tunnels Secure Electronic Transaction (SET) Secure Multipurpose Internet Mail Extensions (S/MIME) Simple Key management for Internet Protocols (SKIP)	
File compression		ZIP, ARC, CAB, TAR, TAR.GX, XXE, UUE		Compression FAQ

Category	Transitional	Current	Emerging	Responsibility and References
Geospatial data	FGDC Spatial Data Transfer Standard	Formats: Arc/Info export (.e00) Shapefiles (shp) ERDAS Image files GeoTIFFs .dxf files Coordinates: **IRM 17-1: Standard Coordinate Specifications for Spatial Data Exchange Between Minnesota State Agencies**	OpenGIS simple features compliant data sources	For OpenGIS exchange standard: http://www.opengis.org/ Geospatial data : IRM Standard 17-1:

Table Formatting:

Plain text: Guidelines — strongly recommended for interoperability and full compliance.

Bold underline: Standards — mandatory for compliance.

Definitions:

Transitional: those that are twilight, retired, or soon to be retired technologies, components and methods and should be discouraged from new implementations. This is not to imply that existing systems need be retired or replaced immediately, but that the use of these products and services should not be extended in any future planning and development.

Current: those that are preferred or required and should be used when making design and implementation decisions.

Emerging: those that include near-term directions and options that need continued monitoring to find applicability within the State IT infrastructure. Included are technologies that are not yet fully production-worthy but are potential candidates for prototype implementations. Continued market acceptance and adaptation will likely move these solutions toward the growth phase of the lifecycle, and inclusion in the statewide architecture will become apparent.

Responsibility and References: what party or group is responsible for keeping this item updateas business needs or technology and industry trends evolve, and/or, a URL or other reference to a defining document or standards document that specifies detail for the technology, component or method.

6. Application Architecture

Purpose

Application Architecture identifies criteria and techniques associated with the design of applications for the State's distributed computing environment. These criteria and techniques ensure that applications can be easily modified to respond quickly to the State's changing business needs, as well as to the rapidly evolving information technologies available to support those needs.

Scope

The State of Minnesota relies heavily on computer applications to support its business operations. Since the State's business processes change dynamically in response to both legislation and new demands from citizens, it is important that the State's computer applications are designed to ensure both interoperability and rapid modification.

Principles

1. **Standard design methods:** The use of industry-recognized standard design methodologies in developing applications.

   Rationale

   - Will help create the highest degree of interoperability and reliability in State software applications
   - Consistent methods aid in project management, resource use, cost containment, quality and scheduling
   - Consistent methods help in identifying and documenting business requirements

   Implication

   - Design and development tools and skills are required.
   - Project management tools and skills are required.
   - Modeling tools and techniques are required.

2. **Interoperability:** The ability to have applications and computers from different sources work seamlessly together on and across networks.

   Rationale

   - Key to sharing resources
   - Long-term development costs will decrease

   Implication

   - Up-front development costs will increase
   - A detailed, indexed repository is required for this to work

3. **N-Tier model:** Separating application user interface, logic, data, and their associated processing and repair.

   Rationale

   - Partitioned code is more flexible in response to changes in internal logic, platforms, and structures; this isolates/minimizes the impact of change
   - Easier to support
   - More scalable
   - Supports interoperability

   Implication

   - The code for business logic, data access, and the user interface will be separated
   - Shared components have to be administered

Best Practices

1. **Foster collaboration between business users and technicians:** Collaborative design and development between business users and technicians e.g., Joint Application Development, Rapid Application Development, Prototyping, Iterative Development

   Justification

   - Shorter development cycles
   - Better user buy-in
   - Better quality applications

2. **Use modeling tools:** Modeling tools provide for a standardized view of the business rules and technical requirements. These models will complement the construction of distributed components.

   Justification

   - Industry standard practice
   - Provides consistent view of the business rules and technical specifications
   - End users can understand the design, and see that it reflects their requirements

3. **Consider business process redesign prior to application design**

   Justification

   - Ensures that applications reflect best practices in business processes as well as IT practices
   - Business processes should drive application requirements.

4. **Document application design:** The design of all applications must be documented. Object models, interaction diagrams and other design artifacts record the structure, behavior and interfaces of application solutions.

   Justification

   - These are important deliverables of the development process that can benefit future efforts.
   - Enhances the opportunity to reuse components
   - Reduces the negative impact of personnel changes

- Extends the useful life of applications

5. **Use project management and software development methodologies:** Make consistent and appropriate use of an established, well-documented methodology, which encompasses all aspects of the systems development life cycle.

   Justification

   - Rigorous and well-documented methodologies provide for: communication among team members, common goals, shared objectives, scope management, resource management, schedule management, test management and control, change management and control, documented business and technical requirements.
   - Organizations learn from project to project; this will improve project estimation over time.

6. **Partition application functionality to mirror business processes:** The boundaries between application component functionality should reflect the way work is accomplished in the business unit.

   Justification

   - Interfaces between components reflect business interfaces so there is linkage between the business and IT solutions.

7. **Leverage web browsers as the user interface.**

   Justification

   - Use of a standard Web browser as the client provides the user with a familiar, intuitive interface and significantly simplifies the process for developing and distributing the user interface.

8. **Use asynchronous processing:** Where appropriate, applications should be designed to take advantage of asynchronous communication processing.

   Justification

   - Allows application independence

9. **Adopt coding standards:** Adopt and document coding standards, in all languages, on all platforms. Even the earliest code developed in a project should conform to the standards. They should address (but not be limited to): naming conventions for variables, constants, data types, procedures and functions; code flow and indentation; error and exception detection and handling; organization of source code libraries; source code documentation and comments.

   Justification

   - Coding standards aid in the debugging and maintenance of applications and can enhance consistency across applications.
   - Enhances the opportunity to reuse components

10. **Manage your application development process using version control, configuration management, and release management.**

    Justification

    - Makes debugging easier
    - Enables a distributed development environment
    - Provides a detailed history of changes
    - Supports a rigorous and orderly change management process
    - Enables simultaneous deployment of independent changes

Technologies, Components and Methods

Category	Transitional	Current	Emerging	Responsibility and References
Systems Development Life Cycle framework	Waterfall	Iterative		
Analysis and design techniques	Computer-Assisted Software Engineering	Joint Application Development ▪ Use cases ▪ Prototyping ▪ Business modeling ▪ Technical modeling Re-engineering Rapid Application Design ▪ Prototyping		Unified Modeling Language (UML): http://www.uml.org/ Advanced Strategies, Inc. business modeling: http://www.advstr.com/web/services.cfm
Application Architecture	Monolithic Two-tier	**N-tier** J2EE Microsoft .NET	Pervasive computing	

Category	Transitional	Current	Emerging	Responsibility and References
Development environments and tools	PowerBuilder 8- Lotus Notes Delphi FoxPro	Too many to completely enumerate. A PARTIAL list: Ant CVS Eclipse GEL IntelliJ Microsoft Access MS Visual Studio Oracle Jdeveloper PowerBuilder 9+ SourceSafe Weblogic Workshop WebSphere Studio GUIDELINE: Your development tools should allow you to build applications in accordance with the recommended architecture, using the recommended languages, and following the principles and best practices.		

Category	Transitional	Current	Emerging	Responsibility and References
Programming languages	COBOL AML Pascal C/C++ Avenue	JAVA C# Visual Basic PERL Python	X#	
Database access	Direct access to physical files Heirarchical view manager	ODBC JDBC Structured Query Language (SQL) Native interfaces		
Supported Web technology	ASP Active X CGI	HTML XML Java servlets JSP ASP.NET Web Services ▪ XML ▪ SOAP ▪ WSDL ▪ UDDI		

Table Formatting:

Plain text: Guidelines — strongly recommended for interoperability and full compliance.

Bold underline: Standards — mandatory for compliance.

Definitions:

Transitional: those that are twilight, retired, or soon to be retired technologies, components and methods and should be discouraged from new implementations. This is not to imply that existing systems need be retired or replaced immediately, but that the use of these products and services should not be extended in any future planning and development.

Current: those that are preferred or required and should be used when making design and implementation decisions.

Emerging: those that include near-term directions and options that need continued monitoring to find applicability within the State IT infrastructure. Included are technologies that are not yet fully production-worthy but are potential candidates for prototype implementations. Continued market acceptance and adaptation will likely move these solutions toward the growth phase of the lifecycle, and inclusion in the statewide architecture will become apparent.

Responsibility and References: what party or group is responsible for keeping this item updated as business needs or technology and industry trends evolve, and/or, a URL or other reference to a defining document or standards document that specifies detail for the technology, component or method.

7. Middleware Architecture

Purpose

Middleware facilitates and simplifies communication within and among heterogeneous, distributed application systems. Middleware enables loosely-coupled modular and flexible systems. Middleware also enables service-oriented architecture.

Scope

The focus of this chapter is limited to application communication middleware.

Principles

1. **Message oriented middleware and asynchronous communication:** Message oriented middleware (MOM) is the preferred method to provide asynchronous communication between applications**.** MOM provides an asynchronous interface between software systems. It provides scalable, secure guaranteed delivery of application messages across process or hardware boundaries. MOM provides a means of sending messages without knowledge of the receiving application's current state. It further provides a dialect agnostic mechanism for applications to communicate with each other.

   Rationale

   - The State needs to be able to deliver scalable and modular applications in a distributed object-oriented environment. This requires a loosely coupled highly modularized infrastructure. The goal of the modularization is to allocate functionality where it belongs and forward all requests for that functionality to the appropriate location. To do that in a scalable fashion requires loosely coupled (asynchronous) communication.
   - Messaging technology allows for transparency in locations, databases, and data structures.

   Implication

   - Use of middleware for communication between application tiers and platforms may initially increase up-front development and acquisition costs.
   - Requires enterprise-wide design of messaging architecture to achieve real benefits.
   - Places greater dependence on network or server based security and authorization mechanisms.
   - Increases need for network management and cooperation.
   - Creates new impacts on system components.
   - Requires a wider (possibly enterprise-wide) focus when designing and deploying applications.

2. **Middleware to support logical partitioning:** Message-oriented and Object Request Broker (ORB) middleware technologies is the preferred method to develop and maintain the logical partitioning of applications and databases within N-Tier architectures.

   Rationale

   - Modular design is more adaptive to changes in internal logic, platforms, and structures. It is the interfaces that allow partitioned components to interact well. Message Oriented Middleware-based solutions promote loosely coupled, highly granular solutions.

   Implication

   - Requires a change in how applications are designed and built.
   - Requires enterprise-wide design of messaging architecture to achieve real benefits.

3. **Middleware to integrate legacy applications:** Message-oriented Middleware is the preferred method for interfacing legacy applications to provide connectivity between legacy systems and other applications.

   Rationale

   - N-tier architecture is the preferred means of distributing applications. The tiers of a distributed application often run on different platforms (client, mid-tier application server, database server) and must be able to communicate. The use of MOM and ORB middleware helps to standardize the solutions to heterogeneous communication requirements.
   - It reduces reliance on institutionalized knowledge of legacy systems.

   Implication

   - Reduces integration complexity and total cost of ownership.
   - Extends the lifespan, usability, and reusability of existing systems.

4. **Consistency in naming conventions:** Middleware components and objects must use a consistent naming convention and schema to be most effective.

   Rationale

   - Consistency in naming conventions and schema will facilitate use and re-use of components, thus increasing productivity and uniformity.

   Implication

   - Achieving consistency in naming conventions and schema will require considerable planning, and collaboration between business units.
   - There are considerable dependencies on the activities in the network and collaborative/directory for achieving consistency in naming.

Best Practices

1. **Minimize middleware configurations:** Middleware components and implementation will minimize the number of standardized configurations that are designed for cross-platform deployment and integration.

   Justification

   - Reducing uniqueness in product selection and standardization reduces support and maintenance costs, and simplifies training and skills transfer. This is the most efficient approach to enterprise-wide middleware configuration and maintenance.

2. **Use asynchronous communications:** Asynchronous messaging (MOM, ORBs etc.) products and configurations should be used whenever possible. Synchronous communication will be used if appropriate in the context of the applications; even then, preference will be given to asynchronous communication run in pseudo-synchronous mode.

   Justification

   - Asynchronous communication promotes flexibility and scalability of the application.
   - Messaging technology allows for transparency in locations, databases, and data structures

3. **Broker integration:** Include a design strategy to allow a broker to be easily integrated into the middleware architecture being implemented.

   Justification

   - Brokers simplify applications coding by reducing the need for changes though there will be significant administrative effort in the broker system itself.
   - Easy integration of a broker will facilitate future inter-application integration.

Technologies, Components and Methods

Category	Transitional	Current	Emerging	Responsibility and References
Interapplication Communication See also Web Services in Data Integration Domain	Screen scraping Terminal emulation	Message Oriented Middleware Object Request Brokers Simple Open Access Protocol (SOAP)	Application Platform Suites (APS)	
Asynchronous Messaging		Application Messaging Interface (AMI) (e.g. IBM MQSeries, MQSeries Internet Pass-Thru) Java Message Service (JMS) API	Application Platform Suites (APS)	
Object-based middleware processors	CORBA Interface Definition Language (IDL)	J2EE and EJB See also Application Architecture Domain	Application Platform Suites (APS)	

Object naming standards		IRM Guideline 9-1: A Data Naming Primer IRM Guideline 10-1: A Data Naming Practitioner's Guide		MN Office of Enterprise Technology OET Data Naming Data Naming Practioner's Guide

Table Formatting:

Plain text: Guidelines — strongly recommended for interoperability and full compliance.

Bold underline: Standards — mandatory for compliance.

Definitions:

Transitional: those that are twilight, retired, or soon to be retired technologies, components and methods and should be discouraged from new implementations. This is not to imply that existing systems need be retired or replaced immediately, but that the use of these products and services should not be extended in any future planning and development.

Current: those that are preferred or required and should be used when making design and implementation decisions.

Emerging: those that include near-term directions and options that need continued monitoring to find applicability within the State IT infrastructure. Included are technologies that are not yet fully production-worthy but are potential candidates for prototype implementations. Continued market acceptance and adaptation will likely move these solutions toward the growth phase of the lifecycle, and inclusion in the statewide architecture will become apparent.

Responsibility and References: what party or group is responsible for keeping this item updated as business needs or technology and industry trends evolve, and/or, a URL or other reference to a defining document or standards document that specifies detail for the technology, component or method.

8. Presentation and Accessibility Architecture

Purpose

Presentation and Accessibility Domain identifies criteria and techniques associated with designing and implementing interfaces needed for adaptive deployment of electronic commerce and internet/intranet web applications. Accessibility refers to the non-dependence of geographic location for access to electronic government services and also the minimization of dependence on the ability of the user (visual, aural, or motor impairments)

Scope

This domain covers these categories:

1. The design of user interface and information delivery through a variety of channels; the top layer of the n-tier architecture.
2. User access systems that are not location and ability dependant

Principles

1. **Leverage the Internet:** The Internet, as an information delivery medium, will be the first technology implementation option for new systems and when performing a rewrite or significant maintenance on a legacy system.

   Rationale

   - Allows the consumer anytime anywhere access to information.
   - Provides a consistent presentation method.
   - Reduces total cost of ownership for state operations.
   - Enhances positive public perception and awareness of state services.
   - Implication
   - Requires technical standards in order to reduce the TCO
   - Requires presentation and publishing standards
   - Requires content management standards and policy for information refresh

2. **Separation of layers:** Separate the presentation layer from the content layer.

   Rationale

   - Accessible systems allow the client to process content in the form that best suits the client and user's capabilities.
   - Users of a system are trying to access information, not presentation.
   - Systems that are used specifically for presentation, such as public relations material, should have the content available in an accessible format easy to obtain and use .

Implication

- Needs architecture and design discipline to follow through.
- May need extensive professional education for IT staff.

3. **State Portal:** [Hold definition of the role of the State Portal until determination by the Portal Steering Committee.]

   Rationale

   -

   Implication

   -

4. **Variety of delivery mechanisms:** A variety of mechanisms and interfaces will be necessary for the state to deliver electronic government services to a wide range of devices. These can include electronic mail, multi-media web pages, streaming audio or video, voice response units, wireless transmissions. Terminal devices include but are not restricted to, voice telephones, video receivers, personal computers, cell telephones, personal digital assistants, and kiosks.

   Rationale

   - Provide portable, anytime, anywhere access.
   - Support accessibility standards and architectures.
   - Provide access choice to consumers.

   Implication

   - requires additional design and implementation effort.
   - requires strict adherence to Principle

5. **Ability independence:** Delivery of electronic government services successfully to those of limited abilities is required.

   Rationale

   - Technology is evolving rapidly. New access problems and solutions are appearing on a nearly daily basis.
   - The rapid development of technology makes any determination of current technical feasibility extremely short lived.
   - Many standards contained in this architecture are based upon human need, rather than specific solutions.
   - As technology moves forward, solutions that improve accessibility are always best practices.

   Implication

   - There will be a higher initial implementation cost.
   - Interface updates will be ongoing..

Best Practices

1. **Hardware independence:** Create documents that do not rely on one type of hardware.

   Justification

   - · Pages will be usable without utilizing a mouse, with small screens, low resolution screens, black and white screens, no screens, with only voice or text output, etc.

2. **Legacy applications:** Adapt legacy applications to a browser based front end where applicable.

   Justification

   - Applications will become interoperable throughout the enterprise. Browser interfaces can be intuitive and reflective of industry trends.

3. **Document storage:** Documents should not be stored in and cataloged in a manner that mandates a particular presentation.

   Justification

   - Presentation software will not have to be installed on workstations.
   - Documents can be more easily used among agencies

4. **Remote bandwidth requirements:** Web pages should be designed to present transfer and display on a remote device in a reasonable amount of time over a 28.8kbps channel.

   Justification

   - Users without broadband access will be able to access state information

5. **Browser versions:** Web pages should be designed for Internet Explorer version 5.0 or later and Netscape version 5.0 or later.

   Justification

   -

6. **Uniformity of presentations:** The state's external presentation of information should be uniform in look and feel so as to present the state as one entity.

   Justification

   - Citizens and business users will feel more at home and less confused within the State of Minnesota's web sites.

Technologies, Components and Methods

Category	Transitional	Current	Emerging	Responsibility and References
Accessibility for differing abilities		W3C Web Content Accessibility Guidelines 1.0 State of Minnesota Accessibility Guidelines		http://www.w3.org/TR/WAI-WEBCONTENT/

Web Development Guide Documents		Minnesota Electronic and Information Technology Accessibility		Office of Enterprise Technology
Interface	3270 ASP	HTML DHTML JSP	XML XHTML XSL	
Wireless		WAP		
Web Browser	Internet Explorer Version 3 or prior Netscape Communicator version 3 or prior	Internet Explorer version 4 or later Netscape Communicator version 4 or later	Internet Explorer version 6 Netscape Communicator version 6	
Access channel bandwidth		v.34 async dialup or greater	ISDN BRI DSL 256kbps Cable Modem	
Web mapping		MapServer ArcIMS	OpenGIS Web Mapping Services	

Table Formatting:

Plain text: Guidelines — strongly recommended for interoperability and full compliance.

Bold underline: Standards — mandatory for compliance.

Definitions:

Transitional: those that are twilight, retired, or soon to be retired technologies, components and methods and should be discouraged from new implementations. This is not to imply that existing systems need be retired or replaced immediately, but that the use of these products and services should not be extended in any future planning and development.

Current: those that are preferred or required and should be used when making design and implementation decisions.

Emerging: those that include near-term directions and options that need continued monitoring to find applicability within the State IT infrastructure. Included are technologies that are not yet fully production-worthy but are potential candidates for prototype implementations. Continued market acceptance and adaptation will likely move these solutions toward the growth phase of the lifecycle, and inclusion in the statewide architecture will become apparent.

Responsibility and References: what party or group is responsible for keeping this item updated as business needs or technology and industry trends evolve, and/or, a URL or other reference to a defining document or standards document that specifies detail for the technology, component or method.

9. Collaboration and Workflow Tools Architecture

Purpose

Collaboration technologies enable organizations to create, share, and leverage accumulated information and knowledge across the entire spectrum of government entities and their associated service programs. Collaboration technologies provide the means for people-to-people communication and collaborative work internally among State agencies as well as between State agencies and external entities.

Scope

This domain contains a variety of technologies that allow State staff to work together effectively as teams in development efforts and service delivery to constituents including electronic communication, directory services and document management tools. Topics to be included are:

Email
File sharing
Calendar sharing
Imaging
Knowledge management
Archive management
Document management
Interactive video/audio communications
Enterprise Directory services
Instant messaging

Principles

1. **Collaboration Systems as Enterprise Solutions:** Each collaboration system is to be designed and managed as if it is an enterprise solution.

   Rationale

   - Collaboration systems typically start as local self-contained collaborative applications, then expand in scope and become difficult to support from both an operational and application-development perspective unless they take an enterprise perspective initially.
   - The creation of collaboration systems based upon broader, enterprise considerations is more likely to produce adaptive systems.

   Implication

   - Each agency involved will have to provide time for the collaboration
   - The information will be shared between agencies to permit interoperability between agencies
   - Avoids support and standard issues down the line.
   - Reduce messaging entry points.

2. **Availability of basic services:** A standardized set of basic collaboration services will be provided to all employees as required to meet business needs.

   Rationale

   - Increases productivity.
   - Reduces costs of maintenance.
   - Provides the basis for multi-agency or statewide business initiatives.
   - Provides for universal employee access to information.

   Implication

   - There will be real time information exchange and scheduling

3. **Data and Process Integration and Sharing:** Collaborative systems must be designed, acquired, developed, or enhanced such that data and processes can be shared and integrated across the enterprise and with external service partners.

   Rationale

   - Increases efficiency while better serving customers (e.g. the public, agencies, etc.).
   - Redundant systems cause higher support costs and lack of data consistency.
   - Ensures more accurate and consistent information.
   - Integration leads to better decision making and accountability by individual agencies and the State as a whole.

   Implication

   - Common repositories can lead to information maintenance reduction. Each agency will not need to perform data importation from other agencies

4. **Virtual LAN:** Directory Services will be designed to support the use of the state-wide network as the gateway to secure anywhere, anytime access to information and services.

   Rationale

   - Networks are the essential enabling technology for client/server, Internet, and collaborative computing.
   - To be fully useful and effective, a common directory for internal communication and collaboration should be accessible by everyone.
   - Knowledge workers' increasing need for access to information across the enterprise must be seamless in order to reduce decision-making cycle times.

   Implication

   - Authentication will be an issue

5. **Document Exchange**: When sharing documents externally, use standardized formats to reduce content exchange conflicts.

   Rationale

   - Content exchange is a critical Collaboration Technologies infrastructure component, enabling the exchange of electronic information and data between individual users and groups.
   - Establishing content exchange standards provides flexibility and independence when exchanging documents.

- These standards enable a variety of tools to be used to view documents stored in standard formats.

Implication

- Information and Data from documents will easily integrate between agencies
- Encryption and authentication will be issue
- Workgroup will have to be formed to determine the standardized formats
- Documents will need to be designated as public, private or confidential in accordance with State statute. Access will need to be controlled accordingly.

Best Practices

1. **External Use of Collaborative Systems:** When designing collaborative systems, give consideration to the possible use of that system by people outside the State enterprise (e.g. general public, 3rd party service providers).

   Justification

   - Supports direct access to information by constituents from multiple locations using multiple methods and media.
   - Supports the delivery of training through distance learning technology.
   - Supports collaboration with clients and external service providers.
   - Constituents may be sending confidential information via a collaborative system.

2. **Classification of Content:** When designing collaborative systems (e.g. document management, workflow), the content that will move through the system must be classified according to applicable statutes, policies and regulations pertaining to availability, retention and security.

   Justification

   - Information in collaborative systems is another type of State information that must be managed according to the same principles of stewardship as structured data.
   - The State must minimize the exposure and liability of mismanaging information stored in collaborative systems.
   - To make information easily shared, it must be classified.

3. **Consistent Configurations:** Create a small number of consistent configurations for collaborative systems and directory services to be used across the State.

   Justification

   - The cost of IT personnel is increasing and the cost of hardware is decreasing rapidly.
   - This is the most efficient approach to enterprise-wide infrastructure configuration and maintenance.
   - By constantly ‘tweaking’ the performance of individual systems, a multitude of unique configurations is created, thus increasing support and maintenance costs.
   - Standardized decisions in product selection simplify training, reduce learning curves and maximize transferability of skills.

4. **Risk Mitigation:** When designing collaborative systems, ensure confidentiality and integrity. Email and other file sharing tools require protection through centrally-managed anti-virus and anti-SPAM solutions.

Justification

- Reduces potential damage to state information assets
- Reduces overall cost.
- Reduces the management costs.
- Protects the statewide messaging systems from internal and external threats.

Technologies, Components and Methods

Category	Transitional	Current	Emerging	Responsibility and References
Email		SMTP – RFC822 POP, IMAP [MAPI] Anti-virus Anti-SPAM	ESMTP	
Instant messaging		TBD		
Document attachment to email		MIME S/MIME [MAPI]		
Directory access protocol		LDAP		
Cross platform data encoding and formatting.		XML		
Imaging		TBD		
Interactive video		H.323		
Calendering			iCalendar (RFC 2445, RFC 2446, RFC 2447)	
Information-sharing network technology		Client/server	Peer-to-peer sharing	

Table Formatting:

Plain text: Guidelines — strongly recommended for interoperability and full compliance.

Bold underline: Standards — mandatory for compliance.

Definitions:

Transitional: those that are twilight, retired, or soon to be retired technologies, components and methods and should be discouraged from new implementations. This is not to imply that existing systems need be retired or replaced immediately, but that the use of these products and services should not be extended in any future planning and development.

Current: those that are preferred or required and should be used when making design and implementation decisions.

Emerging: those that include near-term directions and options that need continued monitoring to find applicability within the State IT infrastructure. Included are technologies that are not yet fully production-worthy but are potential candidates for prototype implementations. Continued market acceptance and adaptation will likely move these solutions toward the growth phase of the lifecycle, and inclusion in the statewide architecture will become apparent.

Responsibility and References: what party or group is responsible for keeping this item updated as business needs or technology and industry trends evolve, and/or, a URL or other reference to a defining document or standards document that specifies detail for the technology, component or method.

10. Security Architecture

Purpose

Security architecture defines a way to protect and secure the State's information resources in order to provide an environment in which the State's business can be safely transacted. It identifies criteria and techniques associated with protecting and providing access to the State's information resources.

Scope

This chapter defines security and authentication technology and practices in the following areas:

Security administration
- Policies
- Administration tools
  - Intrusion detection systems
  - Protocol analysis software
  - Vulnerability, scanning, auditing, and penetration testing tools
  - E-mail content filtering and virus scanning systems
  - Network management (LAN/WAN)
  - Wireless access management
  - Video conferencing

Authentication and identification methods

Cryptography
- Private and Public Key infrastructure
- Digital signature
- Virtual Private Networks (VPNs)

Access Control
- Perimeter security
  - Firewalls
  - Intrusion detection

Internal Security

Privacy and confidentiality

Data Practices Act

Principles

Security Administration

1. **Scale of effort:** Apply a level of security to resources commensurate to its value to the organization and sufficient to contain risk to an acceptable level.

   Rationale

   - Security is a business enabler with associated costs. Security costs should be rationalized to the intended benefits.
   - Requirements for security vary depending on the information system, connection to other systems, sensitivity of data, and probability of harm.

   Implication

   - A business-driven risk assessment for all automated systems must be performed when designing or purchasing new applications.
   - Security costs potentially increase beyond the value of the assets protected. Don't use more security than is required.

2. **Security policy linkage:** All security-based technology deployments and practices must be driven by and in compliance with the written security policy of an individual agency, operational group or the enterprise as a whole.

   Rationale

   - The most important part of a secure system design is to identify the assets that need protection, the level of protection required, and the practices necessary to assure that protection

   Implication

   - A set of security domains must be established and each agency, the State as a whole, or other appropriate entity must create and publish a security policy for that security domain.

3. **Open and industry standards:** Base application security on open standards where possible, industry standards when practical.

   Rationale

   - Security services will be provided as infrastructure services. In order to take advantage of security services, application security must be designed for open standards. A clear migration path should be defined for products not yet capable of integrating with the infrastructure security services.
   - Proprietary products from vendors are often implemented in ways that make it difficult to integrate these products into an overall security architecture.

   Implication

   - Clear identification of integration issues should be part of the design process. If necessary, a migration path should be defined. Selection criteria must include:
   - Adherence to open standards, such as X.509v3 Certificates, SSL, S/MIME, LDAP.

- Adherance to industry standards such as NIST (National Institute of Standards and Technologies), ISO (International Standards Organisation), and COBIT (Control Objectives for Information Technology).
- Avoiding platform-specific implementations that inhibit integration.

Cryptography

1. **Public key infrastructure:** To enable truly reliable and secure electronic commerce and delivery of electronic government services where identification and authentication is needed, an enterprise-wide public key infrastructure, centrally deployed, administered and maintained, is required.

   Rationale

   - Collaboration and co-operation will be required to support security services across the enterprise.
   - A unified approach to a Public Key infrastructure enables the state to respond to changing requirements and conditions.
   - A fragmented approach to a public key infrastructure will complicate administration and management of security across the enterprise.

   Implication

   - The deployment of a public key infrastructure with identified registration authorities; certificate authorities and supporting systems must be a high priority.
   -

Best Practices

Security Administration

1. Date and time accuracy: An accurate system date and time are essential to all security functions and accountability and must be maintained.

Justification

- The validity of digital signatures and electronic transactions depends on precise, reliable date and time information.
- Audit accountability relies on placing events sequentially according to date and time.

2. Communications layer placement: Locate security in the appropriate layer of a communications protocol to ensure maximum usability with minimum future modification.

Justification

- Choosing the appropriate layer in a communications protocol will maximize usability and minimize future changes.
- Security services can have an impact on developers. For example, services provided at the transport layer have less impact on application programmers than services that run above that layer.
- Security services can increase reliance on a network protocol. An appropriate choice depends on the communication requirements of the business system.

3. **Activity monitoring:** Provide the capability to monitor all security-relevant activity.

   Justification

   - Establishing accountability and to detect security violations requires the capability to track security-relevant activity.

4. **Security Vulnerability Scanning Tools:** Tools used to audit the configuration of multiple hosts or application systems.

   Justification

   - Vulnerability audit tools such as Nessus, ISS Vulnerability Scanner, CyberCop identify internal configuration vulnerabilities.
   - Helps standardize and maintain security infrastructure against known vendor design errors/bugs.
   - Provides the means to report and coordinate resources to harden agency systems.

Authentication and Identification Methods

Identification is the process of distinguishing one user from all others. Identification techniques provide a means of gaining entry to the state's resources, such as workstations, networks, and applications. Identification is closely linked to authentication. The most commonly used form of identification is the user ID.

Authentication is the process of verifying the identity of a user. Authentication answers the question: "Are you who you say you are?" Typically the method used to authenticate a user is a password, associated with an individual user ID. Techniques of authentication include smart cards, biometrics, and tokens.

1. **Authentication and authorization:** Authenticate users prior to accessing services. Authorize users based on least privilege.

   Justification

   - Allowing only authenticated users to access system resources protects those resources from inappropriate access.
   - Authenticating users is the basis for providing accountability.

2. **Password and token authentication:** Use token based or strong password-based authentication where public key certificates are not feasible.

   Justification

   - Passwords provide the minimal level of authentication acceptable. Token-based systems are preferred over passwords.

Cryptography

1. **Public key technology:** Use Public Key technology when digital signatures are required.

   Justification

   - Digital signatures are central for most electronic business.

     Public Key technology is the most widely accepted form of digital signatures.

Access Control

1. **Philosophy:** The Defense-In-Depth approach combines the prevention of abnormal situations and their degradation with the mitigation of their consequences.

   Justification

   - A set of actions, items of equipment and/or procedures, classified in levels, the prime aim of each of which is to prevent degradation liable to lead to the next level and to mitigate the consequences of failure of the previous level.
   - Commensurate levels of equipment, application, and personnel resources necessary to mitigate the risks involved.

2. **Perimeter Security:** A combination of security equipment, monitoring, and notification to bulwark and manage access to the secure network.

   Justification

   - Perimeter security management is necessary to achieve agency functions while at the same time insuring that private data is not vulnerable to unauthorized access.

3. **Firewalls:** A firewall technology, configured to protect the various network and host-based services of the agency according to its established security policy, should be installed at each agency enterprise LAN external gateway and at the State enterprise external gateway.

   Justification

   - They provide well-established central points for protecting agency assets against intrusion and disruption.
   - Tracking and monitoring of attempted security violations is critical to the prevention of future damage to State assets.

4. **Perimeter Security – Host-based Intrusion Detection:** Security Policy agents that reside on a particular piece of equipment that monitor changes to the system.

   Justification

   - Host based intrusion detection systems standardize security efforts across the enterprise.
   - Host based intrusion detection systems help to provide real-time data to security personnel.

5. **Perimeter Security – Network-based Intrusion Detection:** Scrutinizes network activity reporting suspicious or anomalous traffic.

   Justification

   - Network based intrusion detection systems look for attack signatures or indicators that packets represent an intrusion..
   - Network based intrusion detection systems help to provide real-time data to security personnel.

6. **Internal Security Architecture:** Segmentation of the secured network consistent with the necessary access.

   Justification

   - Zoned or tiered security architecture provides the means to segment access to the necessary function.
   - Segmentation allows greater flexibility without putting the entire secured network at risk.
   - Automated centralized logging, monitoring, and reporting allows consistent security control.

Technologies, Components and Methods

Category	Transitional	Current	Emerging	Responsibility and References
Security Admin: Secure E-mail	Clear text	**S/MIMEv3** PGP	Secure E-mail Gateway (e.g. Tovaris)	
Security Admin: Secure Messaging		SSL v3		
Security Admin: State-wide security policy				IRM Policy 8: Security Policy
Security Admin: Security assessment and evaluation procedure				IRM Standard 16: Computerized Information Resources Security Standards
Security Admin: Wireless bridging, infrastructure, and ad hoc	WEP 802.11b	EAP 802.11g	802.11i	
Security Admin: Vulnerability Scanning Tools		Microsoft Baseline Security Analyzer NESSUS, ISS		
Authentication & Identification: Web-enabled application security		SSLv3 SSLv3 with client authentication		

Category	Transitional	Current	Emerging	Responsibility and References
Authentication & Identification: Logon authentication	Clear text Passwords	Two-factor authentication	Public Key	NIST Wireless Network Security
Cryptography: Public key certificates		**X.509.v3**		
Cryptography: Virtual private networks	Proprietary VPN PPTP L2TP	**IPsec-compliant VPN**	SSL-compliant VPN	
Cryptography: Public key		RSA (1024 bit keys), ECC (160 bit keys)		
Cryptography: Secret key	DES, RC2, IDEA	, **3-DES**, AES,		
Cryptography: Message digest		MD5, SHA-1		
Access Control: Perimeter security	Stateless packet filtering firewall Packet filtering router as appropriate	**Hybrid stateful inspection/application proxy; ICSA-approved**	Firewall technology + intrusion detection	
Access Control: Internal security – Host-based Intrusion Detection		Coordinated host-based system with central logging/reporting		

Category	Transitional	Current	Emerging	Responsibility and References
Access Control: Internal security – Network-based Intrusion Detection		Coordinated network-based system with central logging/reporting		
Access Control: Internal security – Host-based Security Measures		SANS, CSI, NSA, FIPS best practices		

Table Formatting:

Plain text: Guidelines — strongly recommended for interoperability and full compliance.

Bold underline: Standards — mandatory for compliance.

Definitions:

Transitional: those that are twilight, retired, or soon to be retired technologies, components and methods and should be discouraged from new implementations. This is not to imply that existing systems need be retired or replaced immediately, but that the use of these products and services should not be extended in any future planning and development.

Current: those that are preferred or required and should be used when making design and implementation decisions.

Emerging: those that include near-term directions and options that need continued monitoring to find applicability within the State IT infrastructure. Included are technologies that are not yet fully production-worthy but are potential candidates for prototype implementations. Continued market acceptance and adaptation will likely move these solutions toward the growth phase of the lifecycle, and inclusion in the statewide architecture will become apparent.

Responsibility and References: what party or group is responsible for keeping this item updated as business needs or technology and industry trends evolve, and/or, a URL or other reference to a defining document or standards document that specifies detail for the technology, component or method.

11. System Management and Reliability Architecture

Purpose

The Systems Management Architecture section defines the framework for control, monitoring and measurement of the state's distributed information processing systems to assure continuity and reliability of all services that depend upon them. Resources to be managed include the systems, databases, applications, networks, and Internet components necessary to conduct the automated business functions of the state.

Reliability Architecture section, with the aid of management systems, describes those principles and practices that would create an operational environment where:

- Reliability: Life and/or Public Safety Systems should have at least a 99.99% availability measure, public health and welfare systems should have at least a 99.9% availability measure and systems that support internal operations should have at least a 99% availability measure. All systems must be able to maintain their operational and useful status to the respective constituency.
- Robustness: Tolerance to faults is minimized and systems do not fail or fail very infrequently because of inherent design or built-in redundancies or other means so they will function correctly despite exceptional inputs or stressful conditions.
- Recovery: Restoration of operations from minor or major disruptive events is swift and sure.

Scope

System management can be comprised of several areas:

- Monitoring and control of all computational and network components
- Monitoring of the availability and correct working of critical applications
- Monitoring of network segment loads and responses
- Remote central control of computational and network components for configuration and restart

System reliability can consist of strategies for insuring availability using internal logging and auditing, performance monitoring, continuity of operations plans, including strategies for redundancy, hot spares, rapid sparing, and alternate sites.

Consideration will also be given to failure modes and the minimization of the effects of failure. Technology components such as hot-swappable disks, RAID, mirroring, clustering, redundant servers and continuity plans are part of the scope of this domain.

Principles

1. **Enterprise management system:** A single enterprise-wide network monitoring, control, and trouble ticketing system for the Wide Area Network managed by the Department of Administration is necessary to assure the availability of all critical elements. Any supplementary management systems that exist at various agencies are most effective if interoperable with the enterprise management system.

   Rationale

   - Computational or network elements managed by InterTech that are required outside an agency LAN or WAN must be monitored by a central enterprise system to avoid duplication of effort.
   - A central service organization is needed to monitor the availability and performance of all inter-agency systems where the agencies cannot perform that task themselves.
   - As emphasis on enterprise-wide activities increases, systems and networks must also be monitored and managed with an eye to the whole enterprise.
   - Faults will increasingly involve multiple organizations and the need to have an automated process to trade fault and operational information will correspondingly increase.

   Implication

   - All software and hardware elements that must be integrated with those of other agencies or external organizations must be capable of monitoring as to their availability and performance to assure end-to-end availability.
   - Formal procedures must be implemented to permit rapid contact and assured response of all end agencies personnel in time of fault or failure.
   - Procurement decisions on system management tools will have to done on a cooperative basis and not independently.

2. **Proportional cost:** The extensiveness of effort and resources allocated to reliability must be proportional to the value of the asset or service protected.

   Rationale

   - Reliability and continuity planning is a business enabler with associated costs. Reliability and continuity costs should be rationalized to the intended benefits.
   - Requirements for reliability vary depending upon the information system, dependencies of other systems, necessity of timely response to users and probability of fault or failure.

   Implication

   - A business-driven risk assessment for all automated systems must be performed when designing reliability into new systems.
   - Reliability costs can increase rapidly beyond the value of the assets protected such that the use of excessive reliability systems should be avoided.
   - Continuity costs can increase rapidly when recovery strategies are not aligned with the service it is trying to protect.

3. **Element instrumentation:** Effective reliability and capacity methods require the building in of reliable metrics to track the performance and functioning of all inter-agency systems and components and allow proper proactive reliability measures and capacity planning.

   Rationale

   - Reliability and response can often be a function of capacity. Capacity management and planning require measurement.

Implication

- The cost of resources to include instrumentation must be another natural part of all development planning and budgeting.

4. **Continuity plans:** Timely recovery will require all agencies to have a well-designed and comprehensive continuity of operations plan.

   Rationale

   - In spite of all precautions, conditions will occur that require extraordinary efforts to respond and recover from a catastrophic event.

   Implication

   - Serious effort must be applied to creating, testing and continually maintaining continuity plans.

5. **Performance tuning:** Performance tuning for unique/non-standard components should be minimized

   Rationale

   - Tuning for unique/non-standard components is not worth the increased maintenance costs of multiple individual configurations.
   - Performance tuning can inhibit change to more standard mainstream systems by encouraging comfort with the status quo. It is more cost effective to find an equivalent supported product that meets the functionality required by the existing “unique” solution.

   Implication

   - Efforts to improve performance and reliability of older systems must be prevented except to the extent necessary to keep functionality at the minimum level necessary until transition to a new system is complete.

Best Practices

1. **Resolution databases:** Resolution databases that contain solutions to recurring problems should be built to improve quality and contain costs.

   Justification

   - Effort to resolve recurring problems is significantly reduced
   - Education of new personnel is improved.
   - A knowledge base is available to more quickly resolve new problems with similarities to those previously encountered.

2. **Tiers of support:** Multiple tiers or levels of client support should be employed to leverage support resources and provide effective client support.

   Justification

   - The front-line technical support staff can handle most problems. More difficult problems will need quick escalation to additional levels of expertise. A tiered system with defined response times uses limited talent most effectively.

3. **Single point of contact:** All technical support or help desk implementations should have a single point of contact.

   Justification

   - The users are those being served and should not have to expend additional effort to report problems and faults.
   - Simplicity in error reporting helps assure rapid action.

4. **Inventories:** The technical support organization or help desk should maintain inventories of hardware and software configurations.

   Justification

   - The best action cannot be quickly taken without proper knowledge of what is deployed and in what configurations.

5. **Component Instrumentation:** All components should be instrumented or monitored for reliability, performance tuning and capacity planning. The history collected during monitoring will be used for establishing a baseline of performance.

   Justification

   - Reliable service requires adequate capacity. Adequate capacity is not always obvious without extensive monitoring and tracking data.
   - The historical reporting of collected instrumentation can be used for capacity planning and evaluation of changes.
   - Regular and ad hoc reporting

6. Software Backup and Recovery: This should include operating systems, applications, configurations, licensing, and data.

   Justifications

   Businesses will continue to operate smoothly with minimum interruptions

7. Hardware Restoration: This should include maintenance contracts, sparing, failover and off-sites

   Justification

8. Site Planning Document: Mainly for facility planning, electrical, air and network.

   Justification

   Reliable systems require adequate air, electrical and networking capacity

9. **Continuity plan testing:** Test continuity plans annually.

   Justification

   - Without testing a plan at least annually, the documentation created is ineffectual because one will never know if the theories documented in the plan will actually work.

Technologies, Components and Methods

Category	Transitional	Current	Emerging	Responsibility and References
Monitoring and Management agent		SNMP V2 MIB-2		
Device management		(Note: A fully interoperable standard is not yet available for these purposes. But as data sharing and application coupling beome more prevalent, choices must be made that create a greater consistency or interoperable set of management tools.)		
Trouble Ticketing and Help Desk		(Note: A fully interoperable standard is not yet available for these purposes. But as data sharing and application coupling beome more prevalent, choices must be made that create a greater consistency or interoperable set of management tools.)		
Continuity Planning Software		Business continuity relational database product. (Note: A fully interoperable standard is not yet available for these purposes. But as data sharing and application coupling beome more prevalent, choices must be made that create a greater consistency or interoperable set of management tools.)	Vendor hosted relational database product	Office of Enterprise Technology – Business Continuation Management Unit
Recovery Strategies		Hot Site - IBM Recovery Services Hot Site - SunGard Recovery Services Warm Site - State owned and managed partically equipped Intel based site	Geographically separated redundant sites	Office of Enterprise Technology – Business Continuation Management Unit

Table Formatting:

Plain text: Guidelines — strongly recommended for interoperability and full compliance.

Bold underline: Standards — mandatory for compliance.

Definitions:

Transitional: those that are twilight, retired, or soon to be retired technologies, components and methods and should be discouraged from new implementations. This is not to imply that existing systems need be retired or replaced immediately, but that the use of these products and services should not be extended in any future planning and development.

Current: those that are preferred or required and should be used when making design and implementation decisions.

Emerging: those that include near-term directions and options that need continued monitoring to find applicability within the State IT infrastructure. Included are technologies that are not yet fully production-worthy but are potential candidates for prototype implementations. Continued market acceptance and adaptation will likely move these solutions toward the growth phase of the lifecycle, and inclusion in the statewide architecture will become apparent.

Responsibility and References: Which party or group is responsible for keeping this item updated as business needs or technology and industry trends evolve, and/or, a URL or other reference to a defining document or standards document that specifies detail for the technology, component or method.

Appendix A – Lexicon

Critical terminology has been captured and defined in the Lexicon.

Term Definitions

ADAPTIVE **— Able to support a wide variety of applications, and evolve as technology changes.**

AGENCY — **A governmental unit. In the narrowest sense, a governmental unit of the executive branch.**

ATM — Asynchronous Transfer Mode. **A network technology based on transferring data in cells or packets of a fixed size (53 bytes). The cell used with ATM is relatively small compared to units used with older technologies. The small, constant cell size allows ATM equipment to transmit and switch video, audio, and computer data over the same network via permanent or temporary virtual channels.**

BENCHMARK — **A set of conditions against which a product or system is measured. A benchmarking instrument has been developed and implemented to determine the readiness of state and local governments to adopt the national architecture model.**

BEST PRACTICES — **Recommended methods that serve to direct or guide the detailed design, selection, construction, implementation, deployment, support, or management of the architectural framework. They are based on the success story of one or more other parties or the industry as a whole and they are of the nature, "If you're going to do it, this is the recommended way."**

BLUEPRINT **— Plan or guide, commonly used in construction, laid out logically and including essential elements to be addressed and followed as building progresses.**

COMPONENT — **In object-oriented programming and distributed object technology, a component is a reusable program building block that can be combined with other components in the same or other computers in a distributed network to form an application**

CONCEPT SECTION **— Provides the business case for enterprise-wise architecture**

CONCEPT FOR OPERATIONS **— A description at a relatively high level of the participants in information sharing, the information flows involved and the functional requirements at each step of sharing.**

CURRENT (Technologies, Components and Methods) **—** Those that are preferred or required and should be used when making design and implementation decisions.

DATA **— a representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means.**

Discipline - Logical functional areas to address when building the architecture; a branch of knowledge or of teaching.

DOMAIN **— Logical groupings of disciplines that form the main building blocks within the architectural framework**; a sphere of activity, interest, or function.

Digital Government - The electronic delivery of public services via the Internet.

E-BUSINESS **— Electronic-Business or doing business online. The term is often used synonymously with e-commerce, but e-business encompasses more than just buying and selling of products on the Web.**

ELECTRONIC GOVERNMENT SERVICES **— The electronic delivery of public services via the Internet**

EMERGING **(**Technologies, Components and Methods) **— Those that include near-term directions and options that need continued monitoring to find applicability within the State IT infrastructure. Included are technologies that are not yet fully production-worthy but are potential candidates for prototype implementations. Continued market acceptance and adaptation will likely move these solutions toward the growth phase of the lifecycle, and inclusion in the statewide architecture will become apparent.**

ENTERPRISE **— Enterprise represents an organization in total, including all subordinate entities, encompassing corporations, small businesses, non-profit institutions, government bodies, as well as other kinds of organizations.**

ENTERPRISE ARCHITECTURE **— The holistic expression of the enterprise's key business, information, application and technology strategies. It typically consist of current and future state models of Business Architecture, Information Architecture and Technical Architecture.**

ENTERPRISE BUSINESS ARCHITECTURE **— The expression of the enterprise's key business strategies and their impact on business functions and processes. It typically consists of the current and future state models of business functions, processes and information value chains.**

ENTERPRISE TECHNICAL ARCHITECTURE **— A logically consistent set of principles, practices, standards and guidelines that are derived from business requirements and that guide the engineering of an organization's information systems and technical infrastructure.**

ENTITY **— An information-sharing unit. All agencies (see definition above) are entities; so are courts and legislative bodies. Private organizations that share governmental information are also entities, as are private persons.**

GUIDELINES **— Best practices, suggested approaches, or methods intended to provide the means of meeting requirements of policies or standards.**

IETF **—** Internet Engineering Task Force. **The main standards organization for the Internet. The IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It establishes standards via working groups that are encoded into RFCs. It is open to any interested individual.**

INFORMATION **— A collection of data that is cataloged, stored or processed in computers and that can be used to illustrate new facts or concepts or assembled to create new knowledge.**

INFORMATION ARCHITECTURE **— The art and science of organizing information in automated systems to help people effectively fulfill their information needs.**

INFRASTRUCTURE **— The basic, fundamental physical and logical structure of the system that supports the flow and processing of information, determines how it functions and how flexible it is to meet future requirements.**

INTEGRATION **— The ability to electronically access and exchange critical information at key decision points throughout the enterprise.**

INTERNET **— A worldwide network of packet-switched communications networks utilizing Internet Protocol (IP) as the transport mechanism and which allows any attached computer or intelligent device to communicate with any other and which enables a wide variety of applications to be implemented.**

INTEROPERABILITY **— The capability to allow users to readily share data among**

IP **—**Internet Protocol**. Specifies the format of packets, also called datagrams, and the addressing scheme used to transport information over the Internet. Resides at layer 3 of the OSI network protocol stack. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP)**

ISO **—**International Organization for Standardization**, Geneva, is an organization that sets international standards. The U.S. member body is ANSI.**

LAN **—** Local Area Network. **A computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings**

LEGACY SYSTEMS **— An automated system built with older technology that may be unstructured, lacking in modularity, documentation and even source code.**

LEXICON **— Provides a glossary and cross-reference for words that may have multiple meanings. The purpose is to create common definitions to allow for clearer understanding.**

MANDATE **— An authoritative command or instruction.**

MIB **—** Management Information Base. **A database of objects that can be monitored by a network management system. SNMP uses standardized MIB formats that allows any SNMP tools to monitor any device defined by a MIB.**

MIDDLEWARE **— Middleware is systems integration software for distributed processing and for database and user interfaces.**

MODELS **— Representations of information, activities, relationships and constraints.**

NASCIO - National Association of State Chief Information Officers.

PKI **—** Public Key Infrastructure. **A system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction. Reliable PKIs are implemented to ensure secure electronic commerce.**

POLICY **— Strategic guidance that sets boundaries, establishes direction, influences other decisions and prescribes conduct.**

PRINCIPLE **— A statement of preferred direction or practice. Principles constitute the rules, constraints and behaviors that a bureau will abide by in its daily activities over a long period of time.**

PROPRIETARY **— Owned by a private individual or corporation.**

PROTOCOL **— Rules governing transmitting and receiving of data**

RECORD - **a set of data or information that is treated as a unit and inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.**

RFC **—** Request for Comments**. A series of notes about the Internet, started in 1969 (when the Internet was the ARPANET) that are used to establish standard protocols and practices in to be used to implement or operate the Internet. An Internet document can be submitted to the IETF by anyone, but the IETF decides if the document becomes an RFC. Eventually, if it gains enough interest, it may evolve into an Internet standard.**

SCALABILITY **— The ability to use the same applications and systems on all classes of computers from personal computers to supercomputers**

SNMP **—**Simple Network Management Protocol. **A set of protocols for monitoring and controlling a variety of compliant network devices and hosts. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.**

STANDARD **— Specific and mandatory practices or requirements to be followed focusing on results (as opposed to specific methods) and identifying accountability.**

SYSTEM **— A set of different elements so connected or related as to perform a unique function not performable by the elements alone (Rechtin 1991).**

TCP **—** Transmission Control Protocol**. TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery and provides flow control for packet communications between two hosts. It is used with IP.**

TECHNICAL ARCHITECTUR**E** — **See Enterprise Technical Architecture**

TECHNOLOGY — **Tools or tool systems by which we transform parts of our environment and extend our human capabilities (Tornatzky and Fleischer 1990).**

TEMPLATE **— A form, used as a guide, such as a document in which the standard parts are already filled in and the variable parts can be filled in as appropriate.**

TRANSITIONAL (Technologies, Components and Methods) **—** Those that are twilight, retired, or soon to be retired technologies, components and methods and should be discouraged from new implementations. This is not to imply that existing systems need be retired or replaced immediately, but that the use of these products and services should not be extended in any future planning and development.

WAN **—** Wide Area Network. **Computer networks that spans a relatively large geographical area. Typically, a WAN consists of two or more Local-area Networks (LANs)**