(Revised: 11 JUN 2001 2:00 p.m.)
Section 3

Technical Infrastructure

Process for preparing, reviewing, and updating standards and guidelines

Authority

"The Commission shall: … adopt minimum technical standards, guidelines, and architectures upon recommendation by the technical panel …" Neb. Rev. Stat. Section 86-1506(6)

"… The technical panel may recommend technical standards and guidelines to be considered for adoption by the Commission." Neb Rev. Stat. Section 86-1511(2)

Definitions

Standard: A degree or level of requirement that all jurisdictions should use, which would be enforceable by duly authorized entities. With any standard, there will be circumstances that merit exceptions.

Guideline: A statement of general policy or procedure by which to determine a course of action, subject to reasonable situations. Adherence is voluntary.

Overview

Adhering to a sound set of standards for information technology can reduce costs and improve service delivery. Statute requires the Technical Panel to recommend standards and guidelines to the NITC for adoption. Enforcement of NITC standards and guidelines depends entirely upon cooperation of other entities with such authority.

These procedures permit both the NITC Technical Panel and users to propose standards and guidelines. By statute, the Technical Panel may recommend technical standards and guidelines to the NITC. In addition, any state agency, political subdivision, educational institution, or other information systems user in

Nebraska may propose standards or guidelines for information technology. The technical panel will review the proposal and then invite comments from other information technology coordinating bodies, other government agencies, and the public.

Principles

The Technical Panel and NITC shall observe the following principles when recommending and adopting standards and guidelines:

- Data are shared, consistent with security and confidentiality requirements.
- The infrastructure uses advances in technology that are scalable, reliable and cost-effective.
- Design and development of the statewide infrastructure are collaborative.
- The telecommunications infrastructure is based upon open-systems concepts to assure universal access and interoperability.
- Affected entities should have a reasonable time to implement a standard or guideline.
- The NITC should weigh the benefits of a standard or guideline against the cost of implementation.

Format

The format of a standard or guideline shall include the sections listed below. Eventually, a form will be available for this purpose to facilitate the process of proposing and reviewing standards and guidelines.

1. Title and number
2. Date of first adoption
3. Date of last revision
4. Date of scheduled review
5. Status (draft, pending, active, inactive, standard or guideline)
6. Applicability (who it pertains to)
7. Category
8. Description of impact

9. Related Standards
10. Rationale and justification
11. Primary NITC principle addressed

Process

The Technical Panel will solicit initial standards and guidelines from NITC Councils, other coordinating entities, and state and local agencies. The invitation will include a timeframe for receiving notices and making recommendations to the NITC. After the initial round of standards and guidelines, a sponsor may propose a standard or guideline to the Technical Panel for consideration. Proposals should be e-mailed. Sponsors should describe the standard, its applicability, impact, related standards, and provide other justification.

The Technical Panel will review the proposed standard or guideline and determine whether to proceed with further consideration. The Technical Panel may request further information from the sponsor or make changes to the proposal. The Technical Panel will announce and post the proposed guidance on the World Wide Web for review by affected entities for at least 30 days. Comments should be submitted by e-mail to ~~rbecker@cio.state.ne.us.~~info@cio.state.ne.us. The Technical Panel may appoint special review committees to examine the proposal and make recommendations.

The Technical Panel will review the proposal and any comments received. The review will include an evaluation of the proposal's alignment with the NITC Statewide Technology Plan.

The Technical Panel may make further changes or recommend the proposal to the NITC for adoption. If changes are substantive, in nature, the Technical Panel shall provide another 30-day opportunity for comment.

The NITC may adopt, change, or reject any proposed standard or guideline.

State Enterprise Architecture Framework Overview

Purpose

An "enterprise architecture framework" refers to a conceptual structure for guiding decisions on the exchange of information and utilization of shared information technology resources. The framework includes, but is not limited to networks, computer platforms, applications, and enterprise-specific data. The business case for developing this architecture rests on four foundations:

- **Interoperability:** The architecture promotes effective and efficient exchange of information.
- **Better information**: Information shared within the architecture is accurate, complete, and timely.
- **Greater efficiency:** The architecture facilitates and promotes efficient operations and cost effective sharing of IT staff and technical resources.
- **Flexibility:** The architecture allows managers the freedom to use a range of technology options while providing guidance that avoids compromising the goals of interoperability, better information, and efficiency.

Goals

The goals of this undertaking are to:

- Provide guidelines and standards for the use of information technology in the State of Nebraska;
- Support the ability to integrate data and applications across agencies and government entities;
- Enhance information technology investment and purchasing activities; and
- Provide support for the growth of e-government (the electronic delivery of government services).

General Principles

The Technical Panel and NITC shall observe the following principles when recommending and adopting standards and guidelines for a state enterprise architecture framework. The architecture should:

- Facilitate the strategic objectives of the Statewide Technology Plan;
- Support the use of information technology to improve efficiency and effectiveness of all sectors;
- Increase access to information and services for citizens, business, and government, and all sectors, while protecting privacy and security considerations;
- Enable affected entities to leverage existing technology infrastructure investment;
- Use advances in technology that are scalable, reliable and cost-effective;
- Enable affected entities to use information technology as a catalyst to re-engineer current practices and design better ways of conducting the business of each sector;
- Provide for identification of process and resource owners (responsible individuals); and
- Provide for identification or creation of clear lines of authority and responsibility for all processes and technical decisions.

Affected agencies should be allowed reasonable access to the process of developing standards and guidelines. Affected agencies should have a reasonable time to implement applicable standards and guidelines.

The NITC, in concert with process and resource owners, will weigh the benefits of a standard or guideline against the cost of implementation.

Development

The Technical Panel of the NITC will undertake a review of the current architecture. The review will identify problems as well as strengths. In cooperation with the Councils of the NITC, the Technical Panel will identify the important business drivers that

will determine the adequacy of the architecture in the future. The Technical Panel may sponsor studies of specific components and issues pertaining to the architecture. Based on this information, the Technical Panel will develop a state enterprise architecture framework which:

- Categorizes the architecture into useful components;
- Defines the scope of each component;
- Establishes principles to guide the development of each component of the architecture.

The Technical Panel shall recommend technical standards and guidelines to assist implementation of the architecture. The Technical Panel shall recommend policies and strategies to support the transition from the current to the target architecture.

The architecture framework should reflect the unique requirements of different sectors of the state. Preparing the framework should reflect a collaborative effort. A state enterprise architecture framework should not impede the rapid deployment of appropriate technology or establish cumbersome regulations or bureaucracy.

Given the complexity, scope, and changing nature of technology at the statewide level, developing the state enterprise architecture framework must follow an incremental approach that focuses on functional groups with shared interests. The framework should address the goals of interoperability, better information and greater efficiency within and between functional groups.

Components of the State Enterprise Architecture

Application Architecture

Scope

The State of Nebraska, like most large public and private enterprises, relies heavily on computer applications to support its business operations. Because 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 also be able to change rapidly.

Application architecture establishes criteria that will facilitate interoperability among applications, the use of the correct application as a solution for a given need, and the ease of use of the applications. The architecture also identifies design principles allowing an application to be modified in operation or data interface to respond to the State's changing business needs.

Principles

- Applications are developed or acquired in response to business and customer needs.
- Applications should be considered as shared assets.
- Well designed interfaces will allow applications to communicate with users, data resources and other applications.
- Business rules support the business processes that an agency follows. Business rules define what must be done and how it must be done. Applications must correctly reflect and facilitate those rules. As the business processes of agencies change, the applications must be flexibly designed to quickly and correctly reflect the changes.

Application Development Tools

The application architecture should be independent of any specific technology or set of development tools. Its components, interfaces, business rules, and data access code rules should be able to be

implemented with any development tool, in any language, and on any platform supporting the business needs of the application.

Application development tools are critical in both the development and support of applications. Regardless of the tools selected, it is important that each application module be designed to be portable across platforms. Tool limitations can, however, impact trade-offs in an application's design / architecture. The architecture should determine the tool selection, not the other way around.

Application Management Tools

Applications must be managed as carefully as any other business-support infrastructure. Application management tools, therefore, are a necessity, not an option. Managing distributed applications (i.e., client / server applications) is more difficult than managing monolithic applications, because of the complex intercommunication involving more than one component. The application itself is more complex because its operation is dependent upon more infrastructure components (e.g., networks, servers, workstations, software components, and databases).

The application and its use therefore must be managed as a whole. This requires managing each component of the application and all involved infrastructure components. Applications should be designed to facilitate management.

Best Practices

~~(To be developed)~~ **1. Basic Application Development Stages**

a. The User Requirement:

The initial requirement is a description of what the end-user(s) view as their needs and is often a rather un-detailed description. It usually covers the needs in the end-user community in a very uneven manner, with some aspects (such as ease of installation) often overlooked. It often describes some functions (such as a scheduling mechanism) in very general terms, but others (such as a communications protocol) are discussed thoroughly. Good application development will realize that there are often very important requirements that have not been addressed, and they need to be exposed and handled as they arise. The earlier these issues are addressed and

resolved in the process, the better the prospect of delivering a high-quality product within budget and schedule.

b. The Specification:

The next step is to take the sometimes ambiguous, incomplete, and inconsistent requirement and turn it into an almost flawless detailed specification. This is not yet fully possible with current technology, but there are many reasonable ways of proceeding that give a serviceable specification. The specification is the document that describes what the software is to do and the constraints to be imposed on the designers. It should be noted that production of the specification is not limited to a front-end activity, but that the specification will change throughout the life cycle of the system.

c. The design:

Representation describes how the system is structured to satisfy the specification. It describes the system in a high level manner and defines the breakup of the system into major tasks. It describes persistent data objects and their access mechanisms, the important abstract data types and their encapsulation in the heavyweight tasks, and the message structures between the tasks. There must also be some consideration for how the resources are to be allocated and how the performance requirements are to be satisfied.

d. The final development stage:

Is the creation of the source code, object code, resource usage, and initialized data structures. This is the level at which algorithms are represented explicitly so that programmers can write code quickly and efficiently.

2. Basic Application Development System Views

Views are needed to describe the system's intended and actual operation. The views are relevant at each stage of the system's development and are enumerated below.

a. The functional view:

Shows the system as a set of processes operating on data. This includes a description of the task performed by each process, the flow of data between processes, and the underlying math model, if required. The functional view is often the starting point for the design process, since it deals with what the system is supposed to do, relates the system to its environment, and focuses on the needs of the key participants in the development process: customers, users, and developers. Data flow diagrams are often used to portray how the system will function.

b. The structural view:

Shows how the system is put together: the system's components, the interfaces between them, and the distribution and flow of data and control between the components through the interfaces. It also shows the environment and the interfaces and information flows between it and the system. Ideally, the structural view should be an elaboration of the functional view. Each entity in the latter view is decomposed into a set of primitive software components that can be implemented separately and then combined to build the entity. The design process therefore generally converts a functional view into a structural view. However, the structure of a system is influenced by resource constraints that prevent the use of arbitrarily many or arbitrarily large components. The structure is also influenced by certain implementation constraints that require the use of specific types of component , or require that components be connected in a specific manner . The structural view should include a definition of the number and dimensions of entities to allow for resource estimates. Structure charts are often used to describe the systems interaction and flow.

c. The behavioral view:

Shows the way the system will respond to specific inputs: what states it will adopt, what outputs it will produce for each combination and time sequence of inputs and state transitions, what boundary conditions exist on the validity of inputs and states. This includes a description of the environment that is producing the inputs and consuming the outputs. It also includes constraints on performance that are imposed by the environment and function of the system. Real-time systems especially have performance requirements as an essential part of their correct behavior.

The behavioral view should include a definition of the expected workload and the required responses of the system to this workload. Ideally, the behavioral view should complement the functional view. Each transaction in the functional view should be traceable through the system from the initial input through the interfaces and functional units to the final output.

3. Access to common data.

Duplicative data collection processes exist all across the state government enterprise. An inventory of agency business processes will most likely find numerous instances of agencies collecting the same data for different analytical purposes. Efficiency could be greatly increased if all agencies could access a common database that provided them with this needed information. This has serious customer service and public perception implications as well. The public expects government to have accurate, usable data.

4. Software Development Method

A software development method can provide managers with a series of activities and steps on which they can base schedules and monitor their progress, representations which can be used to document decisions made during development or as deliverables, and rules to analyze representations to support reviews and to judge how complete or correct a group of representations are.

- Does the method provide planning techniques that lead to milestone definitions and project plans that are consistent with use of the method and the implementation language?
- Does the method have analysis techniques that can be used during reviews or that can help you gauge progress during development?
- Are representations clear and easy enough to understand to be used for design reviews?
- Can representations be used to comprise deliverables?

- Can you rapidly develop high-level design representations that can be analyzed to determine the most feasible design approach?

- Does the method prescribe the generation of a sufficient number of intermediate design products to support a detailed project plan?

- Does the method help partition the system into manageable pieces that can be given out to individuals?

- Does the method contain rules that review teams can use to analyze or verify the design?

5. Information "pushed" to users

Agencies must evolve their applications from a "pull" model of information access to a "push" model of information leverage. In the "pull" model, the responsibility is on the service worker to determine the information required and request that information. In the "push" model, the system automatically notifies the appropriate user of a recent event (typically via electronic mail, paging, faxing, etc.) or provides the user with additional information that may be useful (e.g., providing a law enforcement officer with an arrest history during a traffic stop).

- As agencies think of more efficient ways to conduct business, we can take advantage of the benefits of new technology. This necessitates that both I/S staff, program managers, and end users think differently about how applications behave.

- Technology advancements have enabled this paradigm. In the past, the technology to support the push model was not available.

6. Implement client/server systems

Implement application systems using a client/server model in which a desktop processor (client) employs a graphical user interface (GUI) to share application processing with a server(s) over a LAN.

- This is a `thin' client model. It improves system management since the application logic is on the server, not on every client.

- Design application systems for N-tier processing, but deploy the application on two physical platforms whenever possible. The application processing and

database accesses should be on one physical platform and the user interface on the other physical platform.

7. Redefine the role of the programmer

Redefine the domain of the programmer. This is necessary so that rapid, architected application development for both new requirements, as well as for changes to existing systems, can be achieved.

- This allows a division of labor, so that programmers will no longer have to be expert in all areas. Special programmers' skills can be targeted to specific types of programming:

  - User interface: implemented using prototyping and GUI tools.
  - Business rules: implemented using C, COBOL, or a 4GL.
  - Data access: implemented using SQL.

8. Implement open systems

Implement a consistent architecture, based on product, market, and industry standards, in order to achieve the objectives of *open systems*.

- 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.

Standards must be enforced by line managers who understand the importance of consistency in order to facilitate change. Standards cannot be successfully enforced by I/S alone.

9. Web-enabled Applications

There are two primary types of Web-enabled applications. Some Web-enabled applications are used to provide information to clients in page format using HTML and XML to manage content dynamically. Other Web-enabled applications provide fully interactive functionality and near real-time transaction processing capabilities.

Web-enabled applications are a special case of client-server applications where the "client" is a standard Web browser like Netscape Communicator or Microsoft Internet Explorer. The browser serves as another type of user interface (thin client) in the 3-tier or N-tier application. Use of a standard Web browser as the client offers the opportunity to provide the user with a familiar,

intuitive interface and significantly simplifies the process for developing and distributing the user interface.

Ideal Web-enabled applications for the state are N-tier service oriented applications that make use of:

- An industry standard Web browser as the thin client;
- Intranets to provide secure access by state users;
- Extranets to provide restricted access by selected state business partners; and
- The Internet and firewall technology to provide managed access by citizens and other interested parties.

Web-enabled applications will continue to grow in importance to the state as a mechanism for the timely and cost effective delivery of information to the state's employees, business partners and citizens.

10. Application Development Tools

Application architecture should be independent of any specific technology or set of development tools. Its components, the interfaces, business rules, and data access code, can be implemented with *any development tool* in *any language* on *any platform* supporting the business needs of the application.

Application development tools are critical in both the development and support of applications. Regardless of the tools selected, it is important that each tier be designed to be portable across platforms. Tool limitations can, however, impact trade-offs in an application's design/architecture. The architecture should determine the tool selection, not the other way around.

There are three approaches for selecting tools to develop client/server applications:

a. ***Best of breed***. Separate, specialized tools are used for each tier of an application. Middleware must be used to support communications between the different tiers.

b. ***Front end/back end***. Two different tools are used: a specialized user interface development tool and an integrated tool set that also provides middleware for the business rule and data access tiers. Middleware must be used to support communications between the user interface and other two tiers.

c. Integrated. Integrated tool sets, or CASE tools, are used that generate code for all tiers of the application. These tools provide the middleware necessary to support communications between all tiers of the application.

With the *N*-tier service-oriented application architectures, two additional types of tools are required:

- Repositories, or libraries, to keep track of business rules that have been automated by components.
- Software management tools that provide version control, configuration management, and software distribution services.
- There is no "one size fits all" tool set that addresses the needs of all applications or that can be implemented on a statewide basis. The infrastructure of the Statewide Technical Architecture provides flexibility and choices for application development.

The selection of application development tools and intra-application middleware products is up to individual agencies -- as long as they support future external calls to the state's middleware software for inter-application communications and access to shared services.

Standards and Guidelines

(To be developed)

~~Collaboration and Workflow Architecture (Groupware)~~

~~Scope~~

~~Collaboration and workflow architecture establishes a foundation for collaboration, communication, and workflow. Collaboration and workflow focuses on office and ad hoc workgroups, while communication focuses on sharing information both within and outside the state. Components of the architecture include:~~

- ~~Electronic mail~~
- ~~Content exchange~~
- ~~Calendaring and scheduling~~
- ~~Imaging systems~~
- ~~Workflow~~
- ~~Enterprise application software~~

~~Issues related to groupware~~

~~Central to the issue of groupware in the office environment and workplace are the fundamental changes that are occurring in the nature of business in the year 2000. These changes, combined with the impact of globalization, increasing competition, and the virtual enterprise are resulting in new work processes and environments, new models of organizational structure, emerging virtual enterprises, and changes in the nature of work. The traditional office as the workplace is becoming obsolete. In its place is emerging a model for an electronic workplace and a foundation built on Internet standards and intranets.~~

~~The office of the future will see the integration of office systems and groupware capabilities coming together with core applications of the business to create a seamless, user-role-defined workplace environment.~~

~~Compounding the problem, according to the Gartner Group, is that five years is the maximum feasible useful life assumption for electronic workplace architectures. Further, it is suggested that three years be used for most elements.~~

~~Selecting the most appropriate electronic workplace implementation approach, and choosing the best technical strategy, demands different approaches from different organizations. Six different electronic workplace evolutionary~~

~~stages are found across organizations. According to the Gartner Group, different organizations within a single enterprise are often at different levels.~~

- ~~Stage 1: Unconnected. Many organizations continue to base their core workgroup communication on physical office principles. Collaboration occurs in meeting rooms, hallways and via the telephone. PCs are often in place, but electronic information continues to be shared via "sneaker-net".~~
- ~~Stage 2: Externally connected. These organizations use Internet ISPs as the primary internal electronic communication tool.~~
- ~~Stage 3: LAN-based. Deployment of new core business applications (e.g., order tracking) often provides the impetus to interconnect, giving users access to the new application and shared resources.~~
- ~~Stage 4: Chaos. Enterprises continually add to their electronic workplace capabilities. Applications and connectivity expands, bringing WAN-based links between LANs and introducing new capabilities, which often do not integrate well with other systems. Users create new uses and applications, often as application macros.~~
- ~~Stage 5: Single technology standard. Organizations rarely develop and implement a coherent, integrated strategy until the pain and difficulty of chaos exceeds a very high threshold. Well before the pain threshold is hit, distributed organizations often develop their own IS staff - or bring in outside expertise to handle IT operations and planning. Often, only when the pain threshold has been exceeded, will the primary IS group earn the organizational power to develop and implement a strategy to reduce cost, increase efficiency, and improve reliability, integration and other key areas (i.e., the start of a single technology strategy).~~

~~STAGE 6: PLURALISTIC STANDARDIZATION. THESE ORGANIZATIONS ACHIEVE A BALANCE BETWEEN RELIANCE ON SINGLE VENDOR-CENTRIC STRATEGIES AND MORE OPEN APPROACHES WITH VENDOR-INDEPENDENT, STANDARDIZATION MODELS. GENERALLY, NO SINGLE TECHNOLOGY-SPECIFIC STRATEGY WILL SUFFICE FOR ALL SITUATIONS.~~

Accessibility Architecture (Technology Access for Individuals with Disabilities)

Scope

The new standards will provide technical criteria specific to various types of technologies and performance-based requirements focusing on the functional capabilities of covered technologies. Specific criteria cover software applications and operating systems; web-based information or applications; telecommunications functions; video or multi-media products; self contained, closed products such as information kiosks and transaction machines, and computers. Also covered is compatibility with adaptive equipment people with disabilities commonly use for information and communication access.

Principles

(Under development)

See Assistive Technology Work Group
http://www.nitc.state.ne.us/tp/ (click on "Work Groups")

See also http://www.access-board.gov/news/508-final.html

Best Practices

(To be developed)

For some sample guidelines for best practices see
IBM http://www.ibm.com/able/guidelines
Microsoft http://www.microsoft.com/enable/dev/web/
Web Accessibility Initiative http://www.w3.org/wai
Lynx http://lynx.browser.org/

Standards and Guidelines

Nebraska Technology Access Standards

The intent and purpose of these standards is to ensure that the needs of Nebraskans with disabilities are met through reasonable accommodation of the information technology products and services of the state. Future information technology products, systems, and services including data, voice, and video technologies, as well as information dissemination methods, will comply with the following standards to the greatest degree possible.

1. Effective, interactive control and use of the technology including, but not limited to, the operating system,

applications programs, and format of the data presented must be readily achievable by individuals with disabilities.

The intent is to make sure that all newly procured information technology equipment; software and services can be upgraded, replaced or augmented to accommodate individuals with disabilities.

2. Information technology made accessible for individuals with disabilities must be compatible with technology used by other individuals with whom the individual with a disability must interact.

3. Information technology made accessible for individuals with disabilities must be able to be integrated into networks used to share communications among employees, program participants, and the public.

4. Information technology made accessible for individuals with disabilities must have the capability of providing equivalent access to telecommunications or other interconnected network services used by the general population.

5. These provisions do not prohibit the purchase or use of an information technology product that does not meet these standards provided that:

   a. there is no available means by which the product can be made accessible and there is no alternate product that is or can be made accessible; or

   b. the information manipulated or presented by the product is inherently unalterable in nature (i.e., its meaning cannot be preserved if it is conveyed in an alternative manner).

   c. the information technology products or services are used in conjunction with an existing information technology system, and modifying the existing system to become accessible would create an undue burden.

   d. the agency is able to modify or replace the information technology product with one that will accommodate the needs of individuals with disabilities.

When development, procurement, maintenance, or use of electronic and information technology does not meet these standards, individuals with disabilities will be provided with the information and data involved by an alternative means of access.

Groupware Architecture

Scope

The Groupware Architecture establishes a foundation for collaboration, communication, and workflow. Components of the architecture include:

- Electronic mail
- Directory services
- Calendaring and scheduling
- Imaging systems

Principles

The following principles should be followed for Groupware:

- Effective use of groupware requires a consistent infrastructure and communications backbone;
- Groupware technologies must demonstrably overcome time and distance barriers;
- A mechanism must be available to modify standards in a controlled and testable manner as technology and user needs change and advance.

Best Practices / Standards and Guidelines by type of Groupware

Groupware - Directory Services

Directory services allow users to access resources and services across the network regardless of their location or platform. They provide a central view of all available resources on the network, as well as facilitating authentication, access control facilities, and navigation. They provide network users and administrators with transparent access to all network resources, including users, groups, printers, servers, and other physical network devices throughout the network.

In the case of sensitive data (personnel, proprietary, law enforcement, etc.) directory structures including sub folders and file names, shall be protected by an access authorization and

authentication scheme as robust as the protection provided to the directory's contents.

~~**Best Practices.** (To be developed)~~

Standards and Guidelines. ~~(To be developed)~~The Directory Services Workgroup is developing standards and guidelines for state government. More information is available on the NITC Web site at: http://www.nitc.state.ne.us/sgc/workgroups/directory/

Groupware ~~Communication~~ - Electronic Mail (E-mail)

~~The state has a growing need to communicate across agencies, necessitating compatibility between agency e-mail systems. Despite e-mail compatibility problems, e-mail is quickly overtaking traditional voicemail and interoffice mail as the primary means of office communication. While voicemail enables immediate messaging and is accessible from most locations, it does not allow attachments or an organized method of filing messages. External and interoffice mail can be slow and fosters an inefficient, paper-intensive environment, with no capability to share information electronically.~~

E-mail is a mission critical communications~~technology. As such, it requires a consistent, centrally managed infrastructure. By establishing central management of e-mail, it positions the state for implementing emerging e-mail standards, such as guaranteed message delivery.~~

~~The telephone is an example of how a centrally managed system greatly benefits an organization. Telephone systems are not managed by each geographic location; they are managed centrally by a telephone system provider. Each user of the telephone system can choose their individual handset options, including features such as redial, hold, and mute buttons. Similarly, business organizations should be able to choose their own email client software because some users may require more features than others.~~

~~There may be good reasons for an agency to have its own e-mail system for security reasons. This should be allowed as long as state standards are followed for interoperability.~~

~~**Best Practices.** Since delivering Groupware services to citizens~~technology and requires inter-agency ~~cooperation, agencies must have~~cooperation and compatible communications

systems. A statewide email infrastructure facilitates communication on an enterprise-wide basis.

~~For a statewide implementation, the~~**Best Practices.** The state must implement an email architecture based on the following best practices:

- Manage e-mail servers as a statewide infrastructure;
- Allow the attachment of supporting documentation such as word processing documents, spreadsheets, images, etc;
- Support multiple email clients with standard, industry accepted applications programmer interfaces (API's) and integrated (or integratable) security features for authentication and encryption;
- Use a common e-mail directory service;
- Plan for adaptability;
- Implement security for email message transport and storage.

Standards and Guidelines. ~~(To be developed)~~
In November 1997, the Information Resources Cabinet (a coordinating body for information technology in state government which was the predecessor to the NITC) adopted e-mail standards for state government. These standards can be found at http://www.nitc.state.ne.us/sgc/documents/ems.htm.

The State Government Council established the E-mail Work Group to periodically review and make recommendations on e-mail standards for state government. Information on the E-mail Work Group can be found at http://www.nitc.state.ne.us/sgc/workgroups/email/.

~~Collaboration~~Groupware - Calendaring and Scheduling (C&S)

Best Practices. The following best practices should be followed when selecting a C&S application:

- Select an "open systems" C&S application;
- Allow users to create their own groups and lists;
- Enable task and resource management;
- Allow remote and proxy access;
- Allow access via the web;

- Allow modification restrictions and access limitations to be assigned by system administrators and/or users.

Standards and Guidelines. ~~(To be developed)~~
The E-mail Work Group, established by the State Government Council and referenced above, has also been tasked with making recommendations on standards and guidelines for calendaring and scheduling. Information on the E-mail Work Group can be found at http://www.nitc.state.ne.us/sgc/workgroups/email/.

~~Collaboration~~Groupware - Document Management

Groupware products in the form of "office automation suites" have come to embody the typical user's view of sharing work by allowing the creation and exchange of many different types of electronic documents. These documents include those created with word processors, spreadsheet and presentation software tools. In most local area networks (LANs) there are common areas where electronic documents can be stored and accessed by users, if they know where to look for them.

The ubiquity of the scenario described above is beginning to place a large burden on many organizations. Thousands of electronic documents are being created and shared daily. They exist within the file systems of LAN servers and user desktop computers (PCs) and often have cryptic names within a long "pathname" -- the directory names the user must know to locate the filename of the document they need. Most users manage documents through their own naming and filing conventions using operating system and application embedded file managers. From the view of the state as an enterprise, the problems created are manyfold:

- There are too many documents to manage effectively through ad-hoc individual practices. Finding documents or even knowing if they exist is difficult.
- Accountability for the creation or modification of documents does not exist; there is no version control.
- There is little formal structure for the routing and processing of documents.
- There is a need for description standards and mechanisms to facilitate searches and life cycle management.
- Approval and review processes are not well documented
- There are no consistent processes for backing up, cataloging and archiving documents.

Best Practices. It is essential that an organization devise a document management / groupware strategy as an information "architecture" rather than as just another application. This means planning beyond a single stand-alone application. Recognize that electronic document management (EDM) is not necessarily about "imaging". There are real problems with simply managing and sharing the documents created with ordinary word processors and other office automation programs used in the day to day administration of any office. The following points suggest "best practices" related to document management:

- Evaluate potential requirements over a longer-term basis and implement a "platform" that can be used to develop document enabled applications and provide a uniform approach to document storage and access.
- Assure the availability of open application program interfaces.
- Define business processes as conversational procedures, not according to information / data flow.
- Be prepared to modify processes based on lessons learned.
- Match the selected tools to the mission requirements.
- Select EDM and workflow tools that comply with open standards, are platform independent, and can be shown to be interoperable with similar tools and components.
- Select tools that enable reporting of production statistics, real time monitoring of work-in-process, and that provide reporting for longer term process performance metrics.
- Consider the need, cost, and resources associated with the conversion of records backfiles, either on paper or on microfilm / fiche.
- Provide mechanisms for backing up work in progress documents as well as for long term cataloging and archiving of completed documents.

Standards and Guidelines. (To be developed)

Data and Information Architecture

Scope

The data and information architecture provides high quality, consistent data for online transactional processing, where and when it is needed. The architecture also provides standards for accessing data for either public access or online analytical processing, including executive information systems and decision support systems. Components of the architecture include:
(To be developed)

Principles

Principles are relevant to both statewide and agency-wide data. The following principles apply to the Data Architecture:

- Data is an asset that is managed to the benefit of the State.
- Data and the associated metadata should be valued and protected.
- The sharing of data and metadata should be facilitated and increased.
- The business and application architecture drives the data architecture.
- Roles should be created to facilitate the management of data and metadata.
- To insure the integrity of databases, separate on-line transaction processing (OLTP) and on-line analytical processing (OLAP) data sources and repositories should be created.
- Data and metadata should be supported in a distributed environment.

Best Practices

~~(To be developed)~~**1. Data Architecture**

Data architecture is a subset of the information architecture. It encompasses the activities of defining, structuring and documenting the data resource as well as maintaining quality. This is generally done via a series of models. Data architecture

also includes the technology required to build and implement these models.

Data architecture, as we define it here, is not just a single, standard set of products and technologies. A data architecture includes methodologies and guidelines for when and how to use such products and technologies. It also provides different choices for different application and data profiles.

The architecture is likened to a "city plan," noting, "the design of a building or an application system is an architectural issue; one set of blueprints can describe the structure in detail because there is one developer. However, it is not always practical to enforce a blueprint for a whole city — or for an enterprise IS portfolio — because they are developed at different times by independent organizations ... It is as impractical to mandate one DBMS, one language or one design style for all enterprise applications as it would be to mandate that all buildings in a city use the same layout and the same building materials."

2. Benefits of Data Architecture:

The benefits of building a data architecture are not immediately realized. Payback comes from future application and database development — i.e., increased data sharing and reuse, improved data quality (improved data integrity and consistency), ease of integration and data access, and a reduction in development costs for subsequent applications once data structures are in place. Reductions in unplanned redundancy can result in savings in disk hardware as well as in developing and maintaining programs that copy data from one place to another. This also means a reduction in the complexity of the operating environment, resulting in cost and risk reduction.

3. Architecture Elements:

A data architecture has two elements: a data modeling element (a set of data models and business rules, and under that, the data itself) and a technology element. Data architectures must be developed or selected for three classes of applications. Thus, three different architectures correspond to these classes — transactional applications (operational databases), business intelligence applications (data warehouses and data marts) and operational decision support applications (operational data

4. Data Modeling:

The data modeling element consists of a logical and physical model. The logical model should be developed at a high level and

fleshed out when each subject area is implemented. Initially, the logical model is expressed in the form of a conceptual design. -- a representation of the data requirements and the associated business rules, the entities and the relationships between them, and rules for creating and manipulating data. The next stage is the logical design. -- the transition structure that sits between the pure business-oriented model and the physical structure.

In this stage, attributes are defined in detail (including keys), many-to-many relationships are resolved, constraints (domain and referential) are defined, and user views are mapped to the conceptual data model to ensure all access path requirements are met. This is an iterative process back to the conceptual model, as new attributes and relationships may be defined.

The physical element is the physical data model or database design. In the physical design phase, data models are mapped to tables, foreign keys are defined to support referential integrity constraints, indexes are defined, access paths are tuned for optimal performance, user views are created, the need for stored procedures is determined and such procedures are developed. New data attributes may be added to support the physical implementation, and adjustments to the physical database structure may be made. For example, the database might be partitioned or denormalized to enhance performance, availability and manageability of high-volume online transaction processing systems. The physical data topology deals with how centralized or decentralized the data architecture should be, addressing data placement, data consistency and data sharing issues.

5. Perform design reviews for federated data

Establish a *data review board* to create federated (shared) definitions of enterprise level data and establish a framework for sharing federated data.

- Data used by multiple business units must be commonly understood and consistently referenced by all business users. Enterprise sharing of data can only be achieved by creating federated definitions.
- Federated definitions of data can emerge through the context of projects. An enterprise model can evolve over time through ongoing projects.
- The review board should start with small, achievable, and extremely strategic projects.
- In order to create federated definitions of data, cooperation is needed among the business data owners.

- A framework needs to be put in place that allows for:

  - Centralized management of distributed enterprise-level data.
  - Design reviews of new and existing projects for federated data.
  - Enterprise access to information about federated data.

6. Perform design reviews for projects

Perform data design reviews for new and existing projects to identify and use federated data.

- Design reviews are essential to ensure that enterprise shared data is defined consistently across applications. Design reviews also determine whether data that already exists is consistently defined and not redundantly captured.
- A design review evaluates the data requirements of a project and identifies the following:
  - A data requirement that can be solved by using existing federated data.
  - Data not already identified as federated data should be evaluated by the data review board to become federated data.
- Access should be provided to the proper members of application development projects to reference the federated data repository in order to actively research data requirements.

7. Manage through centralized administration

Manage enterprise-level data and databases through centralized administration. Centralized management:

- Is crucial to the quality and consistency of shared data.
- Requires federated definitions of data shared across the enterprise.
- Requires a quality assurance and quality control process in place for enterprise data.
- Requires design reviews of all ongoing projects. Document the following:
  - Where is this application getting its data?

- - What other applications are getting data from this application system?
- - Is data used by this application defined consistently with enterprise definitions? If not, is there a plan to define the data according to enterprise definitions?

- As decentralized databases are implemented across the organization, centralized administration will be crucial to the quality and consistency of the data. Use of inaccurate and inconsistent data is of questionable value.

8. Use a repository for federated data definitions

Use a repository to store the federated data definitions. The repository should be centrally administered and actively managed.

- A repository is a database documenting metadata (e.g., reusable federated data). (Note that a data dictionary discussed later in this chapter is a repository subset that addresses only data for a particular application database, not metadata).
- Storing federated data in a central repository incrementally builds the enterprise data model.
- The repository must be actively maintained (e.g., changes to metadata occur in the repository *before* the changes occur in operational application systems).
- The repository serves as a primary data administration tool and helps promote data reusability, reliability, and sharing across the enterprise.

9. Identify sources of record for federated data

Identify sources of record for federated data.

- Authoritative business sources for federated data should be identified, documented, and actively maintained in the repository. Authoritative business sources are the business units responsible for the accuracy of the data captured.
- A source of record is an authoritative source for data. Data in a source of record is trusted to be accurate and up-to-date. All other data stores should synchronize to the source of record. The data in record sources must be actively managed and the data model should be verified by data administrators. Tools and quality control

techniques must be applied to the contents of the data stores themselves, in order to ensure the quality of the data.

- If the quality of data is questionable by users for a data source that should be an authoritative source, the data source should be identified as a *source*, but not an *authoritative source*. If a source is identified to have unreliable data and the current system is not adaptable or susceptible to modifications, it may be necessary to migrate the data to a new platform and therefore create an authoritative source. This offers a migration strategy to incrementally migrate data from legacy systems. (Note: If the data is unreliable because of an invalid or inefficient process, it may be necessary to fix the data **and the process** in order to fix the problem.)

- Each application must identify data sources for all data which it does not originally capture. The application capturing the original data is the authoritative source, and is responsible for the quality of the data. All application data models for ongoing projects should be reviewed to ensure that data existing in authoritative systems is reused and not redundantly captured.

10. Perform all updates to the authoritative source of record

Perform all data updates to the authoritative sources, then replicate changes to remote databases if necessary.

- An authoritative source for data is the source of record where data is collected and maintained by the application that owns the data. All other data stores should synchronize to the source of record. All data updates should occur against the source of record through the data access rules that own that data.

- The *N*-tier Application Architecture facilitates the implementation of reusable data access rules.

Standards and Guidelines

(To be developed)

~~Electronic Commerce Architecture~~

~~Scope~~

~~Electronic commerce architecture identifies electronic commerce implementation requirements and browser interfaces required to facilitate transactions on-line and public access to information and services. Components of the architecture include:~~

- ~~Security, including authentication, authorization and encryption services and methods;~~
- ~~Card verification and payment services;~~
- ~~Data interchange methods and standards;~~
- ~~Electronic funds transfer;~~
- ~~Electronic benefits transfer;~~
- ~~Electronic commerce applications;~~
- ~~Global interchange and interoperability standards.~~

~~The major components of the emerging electronic economy are defined below. Each definition includes examples of its scope and content. The definitions are intentionally broad to provide an inclusive framework for planning statistical measures, and to allow flexibility to incorporate continuing changes in the electronic economy.~~

~~**E-business infrastructure is integrated into the total economic infrastructure to support electronic business processes and conduct electronic commerce transactions.** It includes hardware, software, telecommunication networks, support services, and human capital used in electronic business and commerce. Examples of e-business infrastructure are:~~

- ~~Computers, routers, and other hardware;~~
- ~~Satellite, wire, and optical communications and network channels;~~
- ~~System and applications software;~~
- ~~Support services, such as web site development and hosting, consulting, electronic payment, and certification services;~~
- ~~Human capital, such as programmers.~~

~~**Electronic business (e-business) is any process that a business organization conducts over a computer-mediated network.** Business organizations include any for-profit, governmental, or nonprofit entity. Their processes include production-, customer-, and internal- or management-focused business processes. Examples of electronic business processes are:~~

- ~~**Production**-focused processes include procurement, ordering, automated stock replenishment, payment processing and other electronic links with suppliers, as well as production control and processes more directly related to the production process.~~

- **Customer** focused processes include marketing, electronic selling, processing of customers orders and payments, and customer management and support.
- **Internal or management** focused processes include automated employee services, training, information sharing, video conferencing, and recruiting.

Electronic commerce (e-commerce) is any transaction completed over a computer-mediated network that involves the transfer of ownership or rights to use goods or services. Transactions occur within selected e-business processes (e.g., selling process) and are "completed" when agreement is reached between the buyer and seller to transfer the ownership or rights to use goods or services. Completed transactions may have a zero price (e.g., a free software download). Examples of both e-commerce and non e-commerce transactions are listed below.

- Linked electronic devices such as computers, personal digital assistants, webTV, Internet-enabled cellular phones, and telephones linked with interactive telephone systems.
- Networks such as the Internet, intranets, extranets, Electronic Data Interchange (EDI) networks, and telecommunication networks. Networks may be either open or closed.

Computer-mediated networks are electronically linked devices that communicate interactively over network channels. Generally, both electronic devices will be computer-enabled, but at a minimum at least one device must be computer-enabled as in the case of a typical telephone linking with an computer-enabled interactive telephone system. Typically, the interactive link involves minimal human intervention though someone activates the electronic devices, accesses the network, and may even assist with the process or transaction. For example, many e-commerce businesses are providing shoppers with the on-line capability of "chatting" with customer support representatives or even speaking with them through the use of Internet telephony software.

Currently accepted development philosophy

- **The private sector should lead.** The Internet e-business componet should develop as a market driven arena, not a regulated industry. Even where collective action is necessary,

the State should encourage industry self-regulation and private sector leadership where possible.

- **The State should avoid undue restrictions on electronic commerce.** In general, parties should be able to enter into legitimate agreements to buy and sell products and services across the Internet with minimal government involvement or intervention.

- **Where State government involvement is needed, its aim should be to support and enforce a predictable, minimal, consistent and simple legal environment for commerce.** Where government intervention is necessary, its role should be to ensure competition, protect intellectual property and privacy, prevent fraud, foster transparency and facilitate dispute resolution, not to regulate.

- **Governments should recognize the unique qualities of the Internet.** The genius and explosive success of the Internet can be attributed in part to its decentralized nature and to its tradition of bottom-up governance. We should not assume that the regulatory frameworks established over the past sixty years for telecommunication, radio and television fit the Internet. Existing laws and regulations that may hinder electronic commerce should be reviewed and revised or eliminated to reflect the needs of the new electronic age.

- **Electronic commerce on the Internet should be facilitated on a global basis.** The Internet is a global marketplace. The legal framework supporting commercial transactions should be consistent and predictable regardless of the jurisdiction in which a particular buyer and seller reside.

— TECHNICAL STANDARDS. **THE MARKETPLACE, NOT GOVERNMENTS, SHOULD DETERMINE TECHNICAL STANDARDS AND OTHER MECHANISMS FOR INTEROPERABILITY ON THE INTERNET. TECHNOLOGY IS MOVING RAPIDLY AND GOVERNMENT ATTEMPTS TO ESTABLISH TECHNICAL STANDARDS TO GOVERN THE INTERNET WOULD ONLY RISK INHIBITING TECHNOLOGICAL INNOVATION.**

E-Government Architecture

Scope

E-Government is defined as "the use of technology to enhance information sharing, service delivery, constituency and client participation, and governance by transforming internal and external relationships." This includes transactions between government and business, government and citizen, government and employee, and among different units and levels of government.

The fundamental purpose of the e-government architecture is to facilitate implementation of citizen-centric access to information and services and support deployment of other e-government applications. The architecture can reduce the time and cost of deploying applications, while making it easier to integrate information and services.

The e-government architecture consists of three conceptual layers:

- Presentation
- Enterprise Services
- Applications and Data

The presentation layer starts with the state's gateway for access to electronic records. It includes any interface between the user and e-government information and services. Enterprise services are the support systems that are necessary for delivering applications and information to users. The applications and data layer provide the specific information or resources sought and valued by the user.

Components of the Enterprise Services layer include:

- Accessibility
- Availability
- Digital archiving
- Encryption
- Help Desk for State Web Site and Software Developers
- Help Desk for Users
- Integration Services
- Network and virtual Private Networks
- Payments
- Privacy

- Search Engine Tools
- Secure Signatures
- Security
- Shopping Carts.

Principles

The following principles should guide the development of the state's e-government architecture:

- The architecture must promote integrated access and delivery of information and services in a manner that is convenient and easy to use;
- The e-government architecture must support the mission of the agency;
- The e-government architecture must facilitate business transformation to improve customer service, achieve cost savings, and reduce complexity;
- The e-government architecture must promote enterprise requirements including security and privacy, aggregation of demand, efficiencies, collaboration within communities of interest, ease of use, and integration of services;
- The e-government architecture must provide adaptability to accommodate change and permit fast deployment of e-government solutions;
- The architecture must encourage creativity, initiative, and innovation by agencies;
- The e-government architecture must accommodate change in technology and changing requirements.

Best Practices

- No single vendor can provide all of the ~~E-business~~E-government applications, services and supporting IT infrastructure to do it all.
- Enterprises should follow the standards relevant to ~~E-business,~~E-government, i.e., those based on Internet protocols and Web technology, and build flexibility into the architecture so that new applications can be deployed with minimum disruption and cost.
- Expectations must be realistic, and a sufficient budget must be made available to enable the ~~E-business.~~E-government.

- An agency planning to ~~become an E-business~~implement E-government should realize that this process would take between two years and five years for most major organizations.

Standards and Guidelines

~~(To be developed)~~The E-Government Architecture Work Group is preparing best practices, standards, and guidelines. A draft E-Government Architecture Document is available on the NITC web site:
http://www.nitc.state.ne.us/tp/workgroups/egovernment/.

Hardware Platform Architecture

Scope

Hardware platform architecture identifies hardware and associated operating systems supporting ~~applications.~~ applications. . The architecture is intended to facilitate a general understanding of decision-making processes related to hardware managed at the enterprise level and to illuminate appropriate standards and guidelines pertinent to hardware managed by an individual agency, board or commission. Principles and Best Practices are documented with the intention of developing a more unified, seamless hardware infrastructure.

Principles

~~(To be developed)~~• Hardware should be acquired in response to business and customer needs. The documentation of those business needs should include required operational characteristics such as general capacity, required availability, responsiveness, anticipated growth in business, or any other such factor that could influence a hardware selection.

• Hardware investments generally should not be considered independent, one-time events. Hardware typically supports one or more solutions to business requirements that typically grow in size and complexity over time. Appropriate planning for additional capacity and/or replacement of aging hardware assets should be incorporated in the initial decision to acquire hardware.

• Hardware investments should not be considered in isolation from other existing or potential hardware investments within the state. Careful consideration must be given to the almost inevitable likelihood of network connectivity or interaction with other hardware.

Best Practices

~~(To be developed)~~• At an enterprise level, formal forecasting of capacity requirements should be performed frequently enough to ensure that an appropriate hardware computing capacity is present within the state.

• Backup and recovery services should be developed, documented and tested for applications and data resident on any given hardware platform.

• Appropriate customer support and maintenance strategies should be developed in conjunction with hardware acquisition. These strategies should be more rigorously structured as criticality and/or visibility of the business solutions being supported on the hardware increases.

• Agencies should periodically review and evaluate their computing environment to assess compatibility with current and future needs. Needs should be considered first and foremost from the perspective of business requirements within the agency, but should also at least briefly consider a purely technical review and analysis.

• Decisions regarding hardware acquisition should include a cost/benefit analysis. To the extent possible, true cost/savings analysis should be documented. Where needed, analysis of intangible benefits should be as detailed and descriptive as possible.

Standards and Guidelines

~~(To be developed)~~• When implemented, the Nebraska Information System (NIS) will introduce a much more unified set of enterprise requirements for hardware capacity and performance. Individual agencies, boards and commissions should review the guidelines published by the NIS Project and carefully consider hardware purchases with that impact in mind. The guidelines are available at http://www.das.state.ne.us/nis/ - the project's homepage.

• The Information Management Services division of the Department of Administrative Services may occasionally set forth standards and guidelines in the discharge of its statutory authority outlined in section 81-1117. Any such information will be available for review at http://www.ims.state.ne.us – the division's homepage.

Network Architecture

Scope

The Network Architecture defines interconnectivity and provides the communication infrastructure for distributed applications and business locations. The Network Architecture is the design strategy for connecting network elements. This includes physical (bus, star, ring) and logical (ATM, FDDI, Ethernet) network topologies as well as the software protocols (or rules) that enable all the devices to interoperate with one another. Components of the architecture include:

- **Local area networks (LAN).** A data communications system of multiple interconnected data terminals, computers, or devices confined to a limited geographic area consisting of a single building, a cluster of buildings, or a campus type of arrangement. The network does not use common-carrier circuits, although it may have gateways or bridges to other public or private networks.
- **Wide Area Networks (WAN).** A data communications system that serves a large geographic area. WANs are often implemented using common-carrier provided lines. A WAN typically serves as a customized communication "backbone" that interconnects all of an organization's local networks with communications trunks designed to be appropriate for anticipated communication rates and volumes between nodes. The existence of a WAN permits the deployment of file; print, or application servers across the infrastructure to create centrally managed LANs where the close proximity of components is no longer a requirement.
- **Internet**. A global collection of interconnected LANs and computers working in a cooperative manner under the standards and guidelines of the Internet Society.

  The Internet will become the predominant mechanism for conducting business, whether it is business-to-consumer (BTC) or business-to-business (BTB). The term "network-connected" will take on new meanings, with ubiquitous Internet connectivity for developed nations allowing a new wave of telecommuting and remote users, leading to virtual organizations. Internet technologies ~~will~~have become pervasive within our state agencies, ~~but will also branch~~and branches into the homes of consumers and public locations such as libraries, airports and hotels.

In spite of more advanced technologies (e.g., generic digital subscriber line (xDSL) and satellite), analog dial-up via modems will remain the primary mechanism for consumer access to the Internet for the near future.

- **Intranet.** A limited collection of interconnected LANs and standalone computers. An intranet functions the same as the Internet, using the same user interfaces and file transfer protocols. The difference between an Internet and an intranet is that an intranet provides connectivity between specific sites in order to create a pre-determined infrastructure for business units, customers, or designated participants. An intranet is often protected from outside access by a firewall. A firewall typically consists of a router with packet-screening ability that can block traffic between networks or specific host computers.
- **Extranets.** Extranets are the secured extensions of internal business processes to known external business partners using Internet-derived applications and technology. The most common evolution of extranets will be the implementation of intranets to gain operational efficiencies, followed by the extension of intranet applications to selected business partners by deploying an extranet. Extranets will first be deployed to arrive at tactical enhancement at the department or business-unit level, rather than the enterprise level.

  Extranet technologies support a wide variety of E-commerce, collaboration and communication applications, but are still immature. During this early phase, extranets will be implemented to support less-complex business processes and will require proprietary development to fill the gaps in available extranet E-commerce applications. Agencies should consider extranet deployment or participation when they can achieve:
  - A secure environment;
  - Competitive or operational gains;
  - Acceptance by target partners.

Issues Affecting Technology Choices

There are many technologies available at each layer and the determination of which ones to use is not an easy task. "Enterprise Networks" are built based on 1) the specific needs of their user communities, 2) the currently available technologies at each layer, and 3) the available resources to implement and support these technologies.

It is important to understand that Enterprise Networks are necessarily built using a series of compromises. Each technology

must be evaluated not only for its technical merit, but also on its ability to interoperate with other components of the network. For example, the best technology for connectivity equipment may not interoperate well with the best network architecture or two Server Architectures which function well independently may not function well when used together on the same network.

Principles

The following networking principles are provided to guide the planning, design, and selection of network technology and services. The network should be:

- A communications infrastructure;
- Easy to use, transparent;
- Scaleable;
- Manageable and supportable;
- The backbone of a technical architecture;
- Available;
- Based on common protocols;
- Unrestrictive with respect to user access locations;
- Supported by the implementation of security features such as encryption, authentication and authorization.

Best Practices

Best practices assist agency staff in the planning, design, implementation and expansion, administration, maintenance, and support of LANs. They are based on experience and proven results. They employ standards and practices designed to support a uniform LAN.

- Networks must be designed for growth.
- Networks must be designed for manageability and reliability.
- Servers must be configured to minimize interruptions.

Standards and Guidelines

(To be developed)

Security Architecture

Scope

Security architecture includes protection of the physical, intellectual, and electronic assets of the state, including its security policies, network access controls, virus protection, network administration, transaction security, and workstation security. Security components may be embedded as indicated earlier, in the components, which comprise the information system infrastructure. Components of the architecture include:

~~- Audits;~~
~~- Authentication Services;~~
~~- Authorization and Access Control;~~
~~- Identification;~~
~~- Security Administration;~~
~~- Transaction Security.~~

~~Principles~~

~~- Users should be authenticated prior to accessing services.~~
~~- Public Key / Private Key technology should be used for authentication when digital signatures are required.~~
~~- Token-based or strong password based authentication should be used where public key certificates are not feasible.~~
~~- An enterprise-wide public key infrastructure should be employed.~~

~~Implementation concerns~~

~~- Make use of strong password controls for all legacy applications.~~
~~- Make use of industry products for applications requiring public key certificate authentication.~~

~~Best Practices~~

~~- Authorize users based on least privilege.~~
~~- Use appropriate security service levels for each part of the technical infrastructure according to enterprise-wide standards.~~
~~- Use open standards-based security solutions.~~
- Information Security Management Policy

- Access Control Policy
- Disaster Recovery Policy
- Education, Training, and Awareness Policy
- Incident Reporting Policy
- Individual Use Policy
- Network Security Policy

Principles

- Information is an asset. It has value to the organization and needs to be suitably protected.
- Owners of systems must determine how critical and sensitive information is and must adopt and implement comprehensive security programs that offer a level of protection commensurate with the value of the assets.
- Information security systems must provide reasonable protection against unauthorized access, disclosure, modification, or destruction, as well as to assure the availability, integrity, utility, authenticity and confidentiality of information. This applies to all systems that gather, generate and store data.
- Adequate perimeter security and logical security measures must protect against unauthorized access to sensitive information on a government facility, network, or application.
- Each agency must have a disaster recovery plan that will identify and mitigate against risks to critical systems and sensitive information in the event of a disaster. The plan shall provide for contingencies to restore information and systems if a disaster occurs. Information resources must be available when needed. Risks to information resources must be managed.
- A program to maintain effective awareness of information security policy, standards and acceptable practices will exist. Persons responsible for information technology resources must have adequate training on implementing proper security controls for the equipment, software, and networks under their control.
- Agencies and institutions shall prepare procedures for monitoring, investigating and reporting security breaches and incidents. Security breaches shall be investigated promptly and documented. If criminal action is suspected, the agency or institution must contact the appropriate law enforcement and investigative authorities.
- Agencies and institutions must adopt policies governing the use of computer and communication facilities by individuals.

- State agencies and institutions shall manage networks in a manner that insures their proper use, prevents unauthorized access or use, maintains availability and protects the security of information resources. State agencies and institutions shall establish controls that are commensurate to the security needs of the information and computer resources on the network. Controls shall also reflect the security needs of other agencies or institutions connected to the network.

Best Practices

(See Standards and Guidelines below.)

Standards and Guidelines

~~(To be developed)~~The Security Architecture Work Group is preparing best practices, standards, and guidelines. The NITC adopted a set of general policies and standards, which are available on the NITC web site at: http://www.nitc.state.ne.us/tp/workgroups/security/

The Security Architecture Work Group is preparing a detailed set of security procedures that agencies and institutions can customize to meet their individual requirements. Copies of the security implementation procedures will be available on the following web site: http://www.nitc.state.ne.us/tp/workgroups/security/.

Systems Management Architecture

Scope

Systems management architecture defines the framework for efficient and effective management of the state's information processing environment needed to support and enhance the productivity of its systems. Systems management can be subdivided into many disciplines; six important disciplines are listed below:

Help Desk
An integrated support services structure that forms the hub for effectively using and deploying technical systems management components. The support services center becomes the central collection point for client contact and control of the problem, change and service management processes.

Operations Management
Encompasses the coordination of system and network resources throughout the enterprise. Its goal is to provide reliable availability for mission critical systems. It includes job scheduling to coordinate jobs and processes in the distributed environment, fault/event management, configuration management, backup and recovery and automated software distribution.

Storage Management
Governs the creation, maintenance and retention of data, including tape and disk management processes.

Performance Monitoring and Tuning
Performance monitoring measures, evaluates and records status information about computer system devices and processes. Tuning applies planned system modifications in order to improve performance. Performance affects how fast and/or how much data is processed.

Security Services
Risk assessment and protection of the physical, intellectual and electronic assets of an enterprise, including security policies, network access, virus protection, firewalls, NOS administration and workstation security.

Disaster Recovery

Recovery plans and technology that insure the continued operation of critical business functions when productivity is threatened by unforeseen circumstances.

Principles

- Business needs have priority.
- The number of permutations in products should be limited.
- "Unique" performance tuning should be limited.
- Capital investment should be increased to offset support costs.
- Open, vendor-neutral standards should be utilized.

Best Practices / Standards and Guidelines ~~by Discipline~~

~~Help Desk~~

~~**Best Practices.** The following practices are recommended as guidelines for developing a service-oriented Help Desk Architecture.~~

~~- Re-engineer to provide integrated services;~~
~~- Improve perception of services;~~
~~- Restructure help-desk within the organization;~~
~~- Design to support an enterprise model;~~
~~- Provide a single point of contact;~~
~~- Provide multiple levels of support;~~
~~- Define reliable metrics and reports;~~
~~- Design to share information;~~
~~- Build to improve quality and contain costs;~~
~~- Maintain configuration inventories.~~

~~**Standards and Guidelines.** There are currently no industry standards for defining a centralized and integrated enterprise-wide help-desk operation.~~

~~Operations Management~~

~~**Best Practices.** The following practices are recommended as guidelines for developing a Systems Management Architecture for operations.~~

~~- Configure for remote management and support~~
~~- Perform systems management functions remotely~~
~~- Limit customer responsibilities for systems management~~

~~- Design for advance notice of failure~~
~~- Maintain inventories in real-time~~

~~**Standards and Guidelines.** (To be developed)~~

~~**Storage Management**~~
~~**Best Practices.** (To be developed)~~

~~**Standards and Guidelines.** (To be developed)~~

~~**Performance Monitoring and Tuning**~~
~~**Best Practices.** (To be developed)~~

~~**Standards and Guidelines.** (To be developed)~~

~~**Security Services**~~
~~**Best Practices.** (To be developed)~~

~~**Standards and Guidelines.** (To be developed)~~

~~**Disaster Recovery**~~
~~**Best Practices.** (To be developed)~~

~~**Standards and Guidelines.** (To be developed)~~

(To be developed)

Video Architecture

Scope

This section will initially address the specific needs of the synchronous distance learning networks of the state. For these networks, the state will establish standards and a migration strategy for existing distance learning systems. Distance learning entities that intend to use state-owned networks would be required to migrate as circumstances permit per a migration strategy that will be recommended by the Technical Panel and approved by the NITC.

Guidelines will also be provided in this section. Those guidelines would apply to all system that are encoding or transferring video and audio in a digital environment. This section will not set guidelines or standards for transfer of digitized video and audio on networks other than synchronous distance learning networks. There are a variety of transfer methods that might be adopted for asynchronous delivery of digital video and audio. Some general guidelines will be provided in the future for such delivery.

Principles

There are principles that apply to all forms of video and audio encoding and decoding to be considered. When considering such systems, criteria should be established to define the specific needs for the system in question. These criteria should be grouped as a minimum into the following areas:

- The quality of video and audio that is required for the application.
- The amount of bandwidth that will be available to transfer the digital video and audio, and the effect that will have on quality.
- All costs associated with the process and responsibility for them.
- The connectivity required to transfer the video and audio, and the amount of that connectivity that might already exist. This could be decided on issues such as where the source of the information exists and where it needs to go. Consider also if

the video and audio will be sent by the source or retrieved from the source.

- Compatibility between source and destination(s). If that compatibility does not exist, an implementation mechanism must be established.

For synchronous distance learning systems, specific criteria for selection of the future standard have been adopted by the Technical Panel in each of the above areas. These are as follows:

Costs

Site - any uniquely required hardware/software cost at remote sites
Hub - if a hub or central switch is required, hardware/software cost
Operational - maintenance requirements, technicians, connectivity bandwidth, scheduling personnel, etc.

Bandwidth

Minimum quality - rate required for NVCN / Neb*Sat Network 3 like quality
High quality - rate required for full-motion / broadcast quality
Lip readable – rate required for language classes (sound synchronized to video and the motion of the teacher's lips is completely distinguishable)
ASL readable – rate required for American Sign Language (hand movements completely distinguishable)
Flexibility - range of data rates available, and rate agility v. preset rate steps
Negotiation - automatic / manual bandwidth negotiation between points

Connectivity

Ubiquity - supported delivery methods (IP, ATM, dedicated line, PVC, etc.)
Broadcast / multicast - one-to-many without interactivity
Point-to-point - two interactive sites
Teleconference - several interactive sites (MCU/Switch required?)
Dial up / dial out - the ability for an external site to connect into a conference and
not have to be brought in
Latency - amount of delay introduced by the encoding process

Compatibility

Standard type - software standard or hardware standard
Backward compatibility - nature of compatibility
Installed base - How prolific is this standard already?
Life Cycle - ability to upgrade

These are the criteria being used by the Video Standards Workgroup to the Technical Panel to determine what standard to adopt for the synchronous distance learning networks of the state. But for adopting any video and audio encoding scheme, agencies will want to consider protocol issues as well.

Protocols are rules agreed to by the involved parties to allow information to pass from one entity to another. In the case of digital video and audio, each system must encompass four parts: communications protocol, video encoding / decoding protocol, audio encoding / decoding protocol, and ancillary data protocol. Some systems wrap all four under a single title. Others might include two or three out of four. Still others require decisions on each independently.

Consider MPEG-4 as an example. This standard only defines protocols for video and audio encoding / decoding. It is a standard that was developed to be passed along a network using Internet Protocol (IP) for communications, so there are no communications protocols specifically designed into the standard. MPEG-4 is optimized for IP networking in its design, but no specific communications protocol exists within MPEG-4. It does incorporate ancillary data (data that can be sent along with the video and audio). MPEG-2 is a looser example. It was designed to pass over any kind of network. There are no specific efficiencies built into the system to favor IP or any other kind of network. It only defines video and audio protocols, but they are not optimized specifically for IP. There is also no ancillary data incorporated into MPEG-2.

Best Practices

All agencies are reminded that they are responsible to be good stewards over the assets of the state. This means that in considering any video and/or audio encoding scheme, efficiencies must be closely examined. One must balance what systems already exist within the group of users that will be associated within the application, with the need to use the technology and technique that promises to be widely accepted for the foreseeable future.

When selecting a system, agencies should:

- Determine goals of the intended system and the participants in the selection process.
- Determine all standards to be considered.
- If a system already exists, eliminate any standard that does not in some way improve costs or operational efficiencies.
- Establish engineering and economic criteria for each standard to be considered.
- Less efficient standards eliminated based on the established criteria and a short list of final candidates developed for a detailed demonstration study.
- Conduct controlled and detailed demonstrations of finalists. Compare the results.
- Make selection and pass findings through appropriate approval and purchasing channels for your agency.

When designing an implementation plan, agencies should consider the following:

- How to integrate new systems using the new standard into the current system as they come on line.
- How to integrate existing systems into the new standard until replaced or upgraded.
- How to migrate to the new standard when an existing system is upgraded to the new standard.
- Identify the financial impact and ways to minimize it.

Once a system is in use, agencies must determine when to periodically review performance. This review should compare operational projections used to select the system with actual performance. Projected and actual costs should be compared, as well as maintenance requirements. After installation, agencies should continue to watch industry trends. Since no system is permanent, agencies will have to balance getting the longest life

out of a system with not allowing a system to outlive its useful and maintainable life.

Standards and Guidelines

A video and audio encoding standard for synchronous distance learning networks is currently in development. An integral part of that standard is a specific implementation plan that will consider each network partner individually. The current schedule to complete this task is as follows:

Jan 2001 Present goals & participants to Tech Panel for approval.
Feb 2001 Engineering and economic criteria established and standards to be considered established.
Mar 2001 Less efficient standards eliminated and short list for detailed study determined.
Jul 2001 Individual spreadsheets on each standard and its status relating to established criteria. Select finalists.
Sep 2001 Demonstrations of finalists.
Oct 2001 Present findings to Technical Panel for approval. Give demonstrations.
Jan 2002 Create migration / implementation plan and present to Technical Panel for approval.

When the standard is selected and an implementation plan in place they will be added to this document. Guidelines for all other video and audio encoding systems are incorporated into the "Principles" and "Best Practices" sections of this document.