State of New Mexico Statewide
Architectural Configuration Requirement
Title: Enterprise IT Security Guidelines
S-GUIDE-002.003
Effective Date: October 18, 2005

1. Authority

The Department of Information Technology (DoIT) in coordination with the Information Technology Commission, shall develop, implement and maintain a coordinated statewide plan for information technology (IT) including the adoption of statewide technical, coordination, and security standards per the Department of Information Technology Act, NMAC 9-27-1 et. seq. (1978).

2. Purpose

The purpose of this guideline is to establish an Enterprise Security guidelines for the protection of IT assets and resources including data/information, for the State of New Mexico.

3. Scope

This applies to all Executive Agencies and to any other agency or entity utilizing Executive Agency infrastructure.

The Department Secretary or Agency Director, working in conjunction with the Department or Agency Chief Information Officer or IT Lead, shall be responsible for ensuring the effective implementation of Statewide Information Technology Policies, Standards, and Procedures within each agency.

4. Guideline

The State of New Mexico shall securely and economically protect its business functions, including public access to appropriate information and resources, while maintaining compliance with the legal requirements established by existing federal and State statutes pertaining to confidentiality, privacy, accessibility, availability, and integrity.

Security Architecture addresses all relevant criteria on an Enterprise scale, rather than as an individual New Mexico State Agency or part of the deployment of an individual application. New Mexico State Agencies have differing levels of security requirements and statutory mandates. Security Architecture addresses security requirements and statutory mandates to establish a recommended minimum baseline for Security Architecture. New Mexico State Agencies that require higher levels of security based on more stringent mandates will extend or add to the baseline Security Architecture and will document additions accordingly in State Agency policies, standards, and procedures.

4.1 IT Security Policy Responsibilities

The guideline provides recommended actions for New Mexico State Agencies to follow:

4.1.1 Protect the State's IT assets, resources, and data/information from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

- Integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;
- Confidentiality, which means preserving authorized restrictions from access and disclosure, including means for protecting personal privacy and proprietary information;
- Availability, which means ensuring timely and reliable access to and use of information. Availability is securely accomplished through identification, authentication, and authorization and access control;
- Accountability, which includes requirements that actions of individuals or entities can be traced to the individual or entity, non-repudiation, and security review controls and procedures; and
- Assurance, including security administration and adherence to Statewide
- IT security policies and standards.

4.1.2 Provide security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, modification to, or destruction of either:

- Information collected or maintained by or on behalf of the New Mexico State Agency; or
- Information systems used by an New Mexico State Agency or by a contractor of a New Mexico State Agency or other organization on behalf of the State Agency.

4.1.3 Ensure that data/information contained in electronic transactions is protected via:

- Identification, authentication, and authorization;
- Encryption; and
- Electronic signature, as necessary.

4.1.4 Provide adequate security for all information collected, processed, transmitted, stored, or disseminated in New Mexico State Agency software application systems.

4.1.5 Ensure that networks, hardware systems, and software application systems operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

4.1.6 Apply security controls to information systems, resources, and data/information sufficient to contain risk of loss or misuse of the information to an acceptable level that supports the mission and operation of the State Agency.

4.1.7 Ensure that information security management processes are integrated with State Agency strategic and operational planning processes, including planning and implementing *(see paragraph 4.6)* any necessary remedial action to address IT security deficiencies.

4.1.8 Communicate applicable Enterprise and State Agency specific IT security policies and standards to appropriate third-party organizations.

4.1.9 Establish IT security programs, including assignment of roles and responsibilities, as well as creation of any necessary procedures, adherence requirements, and monitoring controls that adhere to:

- State of New Mexico Enterprise Security Policy;
- Applicable New Mexico Statewide Standards for IT security; and
- New Mexico State Agency specific IT security policies, standards, and procedures.

New Mexico State Agency security programs shall be appropriate to each Agency's operational and technology environment in order to provide a foundation for management to make informed decisions and IT investments that appropriately mitigate IT security risks to an acceptable level.

4.1.10 Identify, define, and resolve overlapping IT security roles/responsibilities between New Mexico State Agencies and/or contractors relative to security services received from, or provided to, other New Mexico State Agencies. Security services received from, or provided to, other New Mexico State Agencies should be defined by a Service Level Agreement.

4.2 Security Architecture Principles

The planning, design, and development of Security Architecture are guided by the following general principles that support the State's strategic business goals and objectives.

4.2.1 Security Architecture shall enable the State and its Agencies to perform business processes electronically and deliver secure e-government services to the public.

4.2.2 Security levels applied to systems and resources shall, at a minimum, be commensurate with their value to the State and its Agencies, and sufficient to contain risk to an acceptable level.

4.2.3 Security Architecture shall be based on industry-wide, open standards, where possible, and accommodate varying needs for and levels of security.

4.2.4 Security is a critical component of individual New Mexico State Agency and New Mexico State Enterprise systems interoperability.

4.2.5 Security architecture shall accommodate varying security needs. Supporting rationale for the above principles can be found in the State of New Mexico Framework for Enterprise Architecture Program: http://www.doit.state.nm.us/docs/architecture/FrameworkForEntArchProg.pdf

4.3 Security Architecture Target Technologies

Components of the Target Security Architecture are reviewed and refreshed on a regular and scheduled basis to address major shifts in technology, as well as the emergence and adoption of new technology-related industry or open standards.

4.4 Security Architecture Standards

Security Architecture defines common, industry-wide, open-standards-based technologies required to enable secure and efficient transaction of business, delivery of services, and communications among its citizens, the federal government, cities, counties, and local governments, as well as the private-business sector. Security Architecture Standards allow the State and individual New Mexico State Agencies to quickly respond to changes in technology, business, and information requirements without compromising the security, integrity, and performance of the enterprise and its information resources. Refer to Paragraph 5.0.1, Statewide Standards, for further information.

4.5 Implementation

New Mexico's Enterprise Architecture Framework has been designed to maximize current investments in technology, provide a workable transition path to targeted technologies, maintain flexibility, and to enhance interoperability and sharing. Security Architecture and shall be implemented in accordance with this policy, applicable Statewide standards for security, and relevant Federal, and New Mexico State Agency standards.

4.6 Conformance of IT investments and projects to Enterprise Architecture

To achieve the benefits of an enterprise-standards-based architecture, all information technology investments shall conform to the established Enterprise Architecture that is designed to ensure the integrity and interoperability of information technologies for New Mexico Agencies. Variances from the established Enterprise Architecture shall be documented and justified.

4.7 Compliance to Standard

Non-compliance with this standard may lead to limitation and/or termination of services.

5. Definitions

Refer to the N-DEF001.001 Glossary of Terms located on the DoIT website:
http://www.doit.state.nm.us/standards.html

6. References

Enterprise Architecture, NMAC 1.12.11
Enterprise Architecture, NMAC 1.12.11.15, Network
Enterprise Architecture, NMAC 1.12.11.16, Password

7. Attachments

None

8. Version Control

S-GUIDE-002-003

9. Revision History

Original 10/18/05
Format Updated 09/18/13