State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
119	A	Information Technology Contractors	01/22/2015	1 of 2

1.0 PURPOSE

Establish standard requirements regarding contract IT services provided to the State of Nevada.

2.0 SCOPE

This standard applies to any entity regardless of physical location that utilizes contract services to operate, manage or maintain IT services or equipment.

3.0 EFFECTIVE DATES

This standard becomes effective at the time of approval of the State Chief Information Officer (CIO).

4.0 RESPONSIBILITIES

The agency head and appointed agency Information Security Officer (ISO) have the responsibility to ensure the implementation of and compliance with this standard. The unit managers are responsible for disseminating this standard and implementation within their units.

5.0 RELATED DOCUMENTS

Nevada Revised Statutes (NRS) - Chapter 333 (Purchasing: State)
State Information Security Consolidated Policy, 100
EITS Security Standard 54.174210C, Suspension of Network Service

6.0 STANDARD

A. Fingerprint based background checks must be conducted on all persons contracted for IT services.

B. Any IT service contract must include, at minimum, the following language:

1) All information technology services and systems developed or acquired by agencies shall have documented security specifications that include an analysis of security risks and recommended controls (including access control and contingency plans).
2) Security controls shall be developed at the same time system planners define the requirements of the system. Requirements must permit updating security controls as new threats/vulnerabilities are identified and/or new technologies implemented.
3) Security requirements and evaluation/test procedures shall be included in all solicitation documents and/or acquisition specifications.
4) Security requirements and controls must be identified, incorporated and verified in each phase of system development for approval by the owning agency.
5) The State agency must approve and authorize all changes to any system or service with recommended changes documented to identify the security implications.

6) Application systems and information that become obsolete and no longer used must be disposed of by appropriate procedures. The application and associated information must be either preserved, discarded or destroyed in accordance with Electronic Record and Record Management requirements defined in NRS and NAC 239, Records Management.

C. The Knowledge Skills and Abilities (KSA) of contract personnel who manage devices that have any connection to or impact on the SilverNet infrastructure must be validated by appropriate EITS staff.

D. A security vulnerability assessment of any new contracted IT system / application / network infrastructure is required prior to such a system / application / infrastructure being implemented into production.

E. Any IT contract service or contractor action that violates applicable Nevada Revised Statues (NRS), State, and/or EITS Security policies, standards, and procedures (PSPs) may have services to SilverNet suspended in accordance with EITS Suspension of Network Service standard.

7.0 DEFINITIONS/BACKGROUND

None

8.0 EXCEPTIONS/OTHER ISSUES

Requests for exception to the requirements of this Information Security Standard must be documented, provided to the Office of Information Security (OIS), and approved by the State Chief Information Security Officer (CISO).

Approved By		
Title	**Signature**	**Date**
State Information Security Committee	Approved by Committee	10/27/2011
State Chief Information Security Officer (CISO)	Signature on File	2/21/2012
State Chief Information Officer (CIO)	Signature on File	1/22/2015

Document History		
Revision	**Date**	**Change**
A	2/21/12	Initial Release