State of Nevada

Information Security Committee

Standard

Document ID	Title	Revision	Effective Date	Page
S.4.07.01	Security for Software Development	D	12/31/2020	1 of 3

1.0 PURPOSE

This standard establishes the minimum requirements and appropriate level of security controls for software development.

As state agencies design, build, and deploy information technology-based services, each new project must address the security needed for the effective business operation of the information system. Security controls must be an integral part of project planning, testing, development, and implementation.

2.0 SCOPE

This standard applies to all state agencies meeting the criteria identified in the State Information Security Program Policy, Section 1.2, Scope and Applicability.

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 Information Security Officer (ISO) have the responsibility to ensure the implementation of and compliance with this standard.

5.0 RELATED DOCUMENTS

NRS and NAC 239, Public Records, including
    NAC 239.900-239.945, Records Management
State Information Security Program Policy, 100
Information Security Officer (ISO) Roles and Responsibilities, S.3.03.01
Information Security Risk Analysis, S.3.07.01
IT Contingency Planning, S.3.09.01
Access Controls and Audit Trails, S.5.02.02

6.0 STANDARD

6.1 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 systems and contingency plans).

6.2 Security requirements shall be developed at the same time system planners define the requirements of the system. Requirements must permit updating security requirements as new threats/vulnerabilities are identified and/or new technologies implemented.

6.3 Security requirements and evaluation/test procedures shall be included in all solicitation documents and/or acquisition specifications.

6.4 Security consideration must be included in each phase of System Development.

6.5 Systems developed by either internal State or contracted system developers shall not include back doors, or other code that would cause or allow unauthorized access or manipulation of code or data.

6.6 Security specifications shall be developed by the system developer for approval by the agency owning the system at appropriate points of the system development or acquisition cycle.

6.7 All approved information technology services and systems must address the security implications of any changes made to a particular service or system.

6.8 The responsible agencies must authorize all changes.

6.9 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 Public Records, Electronic Records, and Record Management requirements outlined in NRS and NAC 239.

7.0 DEFINITIONS

None

8.0 RESOURCES

Nevada State Library, Archives, and Public Records (NSLAPR),
Nevada Public Records Act: A Manual for State Agencies

9.0 EXCEPTIONS

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	Approval Date
State Information Security Committee	Approved by Committee	11/19/2020
State Chief Information Security Officer (CISO)	Signature on File	11/24/2020
State Chief Information Officer (CIO)	Signature on File	11/30/2020

Document History

Revision	Effective Date	Change
A	8/08/2002	Initial release
B	8/06/2012	OIS biennial review, replaces standard 4.30
C	12/26/2018	Renumbering (131 to S.4.07.01) and compliance to ADA standards.
D	12/31/2020	Biennial review for alignment with CIS Controls v7.1, Implementation Group 1 (IG1)