State of Nevada

Information Security Committee

Standard

Document ID	Title	Revision	Effective Date	Page
S.6.02.07	System, Application and Service Blacklisting	A	01/26/2023	1 of 3

1.0 PURPOSE

The purpose of this standard is to establish the criteria and methods for establishing and maintaining a blacklist of hardware, software, vendors, and services that are banned from use in the State of Nevada due to security concerns.

2.0 SCOPE

This standard applies to all state agencies and authorized users 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

State Information Security Program Policy, 100

6.0 STANDARD

To ensure the security and privacy of the State of Nevada information and infrastructure, certain hardware and software products, manufacturers, vendors, and services may be prohibited from use on state-owned hardware and state-managed user accounts.

6.1 BLACKLIST CREATION AND MANAGEMENT

A. The State Information Security Committee (SISC) shall establish a statewide blacklist of hardware, software, services, manufacturers, and vendors.

B. Items included on the blacklist shall not be used or purchased by any agency. If an item is already in use by an agency when the item is added to the list, the agency shall submit to the CISO a plan to discontinue its use, including budgetary and operational considerations along with management of the risk until the plan is completed.

C. The blacklist will be maintained by the Office of Information Security (OIS) and published on the Security PSP website.

D. The blacklist can only be altered or amended by SISC as described in section 6.2 of this standard.

E. The statewide blacklist will not preclude agencies from maintaining their own blacklists or whitelists.

i. Agency blacklists will not supersede the statewide blacklist; these lists will be considered additions to the statewide blacklist that apply only to that agency.

ii. Agencies may not whitelist items included on the statewide blacklist.

F. Items blacklisted by the Federal government will be included on the state blacklist by default.

G. The blacklist will only apply to state-owned devices, and state programs and processes. It will not impact state employees' personal use on the employee's personal devices.

6.2 BLACKLIST CHANGE PROCEDURE

A. Any agency may submit a change (addition/deletion) to the blacklist through their ISO or SISC representative.

i. Requests for change should be submitted to the State Chief Information Security Officer (CISO) via email.

ii. Reasons for submission should be related to security or privacy concerns with the product, service, vendor or manufacturer. Examples may include relationship with a hostile foreign government, established insecure business practices, established track record of security violations, or similar.

B. The CISO will add the change to the agenda for the next scheduled SISC meeting for discussion. The agency that proposed the change will be expected to present their reasons for the proposal and answer questions from the committee.

C. The change is then sent to agencies for internal discussion and identification of impact to business processes, agency infrastructure, and budget. Agencies may share concerns via email or other online communications during this review.

D. At the following SISC meeting, agency feedback and concerns are discussed. Unless an agency requests more time for further review, the change is voted on when discussion is ended.

E. Upon an affirmative vote, the change is made to the blacklist. If the change is an addition, the ban on that item goes into effect immediately. If the change is a deletion, the ban on that item is lifted.

i. If the blacklist entry is deleted, it may be added to agency blacklists at the agency's discretion.

ii. The CISO is responsible for ensuring changes to the blacklist are communicated to stakeholders promptly. Stakeholders include all agency ISOs, the State CIO, and State Purchasing.

F. Exceptions for blacklisted items shall be requested via normal exception process.

G. In case of an immediate, active threat, the CISO may institute a temporary emergency ban.

i. The CISO shall communicate the emergency ban to all agency ISOs and the State CIO, with justification for both the ban and the urgency.

ii. The emergency ban will only be in effect until the next SISC meeting. At that time, the emergency ban entry must be voted on to be affirmed (made permanent) or reversed.

7.0 DEFINITIONS

Blacklist – A list of discrete entities, such as hosts, email addresses, network port numbers, runtime processes, or applications, that have been previously determined to be associated with malicious activity.

Whitelist – A list of discrete entities, such as hosts, email addresses, network port numbers, runtime processes, or applications that are authorized to be present or active on a system according to a well-defined baseline.

8.0 RESOURCES

Center for Internet Security (CIS), CIS Controls v7.1 Guide

National Institute of Standards and Technology (NIST) Computer Security Resource Center Glossary

9.0 EXCEPTIONS

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

Approved By

Title	Signature	Approval Date
State Information Security Committee	Approved by Committee	01/26/2023
State Chief Information Security Officer (CISO)	Signature on file	01/26/2023
State Chief Information Officer (CIO)	Signature on file	01/26/2023

Document History

Revision	Effective Date	Change
A	01/26/2023	Initial release