1.0 PURPOSE

This Standard establishes a consistent, statewide approach for executive branch public websites and public-facing domains (web addresses). It is intended to help the public recognize official Nevada government websites, reduce phishing and spoofing risks, and set baseline requirements for security, accessibility, and content governance.

- Make it easier for Nevadans to identify official government websites.
- Reduce risk from lookalike domains and spoofed websites used for fraud or phishing.
- Provide a clear, supported intake process so agencies do not need to improvise when they need a new site or web address.
- Maintain an authoritative directory of official websites for use by agencies and Public Information Officers (PIOs).

2.0 SCOPE

This Standard applies to executive branch agencies and any state employee, contractor, vendor, or third party acting on behalf of an executive branch agency who creates, manages, hosts, administers, or publicly promotes an official Nevada state website or domain.

Includes: This Standard governs both:

- Public websites (including agency/program websites, public portals, and online services).
- Public-facing domains and subdomains used to represent Nevada executive branch services.

This Standard does not apply to internal intranet sites.

Exemptions and special cases are described in Section 7.3 and Section 9.0.

3.0 AUTHORITY

- NRS 242.115 – directs the State CIO/Chief to develop policies and standards for executive branch information systems, excluding NSHE and NCJIS.
- NAC 242.110 – adopts State Information Security Policies, Standards and Procedures by reference for executive branch agencies and relevant third parties.

- NRS Chapter 239 – public records and records retention/disposition schedules applicable to website publishing and related records.

4.0 REFERENCES & RELATED DOCUMENTS

Key references include:

State of Nevada Web Style Standard (Control 4.01).
State Information Security Policies, Standards and Procedures (State Security PSP).
CISA get.gov guidance for .gov eligibility and WHOIS lookup.
CISA Secure Our World – Recognize and Report Phishing guidance and tip sheet.
FBI IC3 public service announcements related to spoofed government websites and search-ad impersonation.
NRS Chapter 239 and State Library, Archives and Public Records retention schedules.

5.0 DEFINITIONS

- Domain: The primary web address used to reach a website (example: agency.nv.gov).
- Subdomain: A child address under a parent domain (example: program.agency.nv.gov).
- Canonical URL: The single official web address the public should use; alternate addresses must redirect to the canonical URL.
- Authoritative directory: The official list of approved executive branch websites/domains maintained by GTO.
- Lookalike domain: A domain intended to impersonate a legitimate domain by small spelling changes or a different top-level domain (example: ic3[.]com vs ic3[.]gov).
- Defanging: A safe way to write a URL so it cannot be clicked (example: hxxps://example[.]com).

6.0 ROLES & RESPONSIBILITIES

- State CIO (Chief/Administrator): Approves this Standard and provides statewide direction under NRS 242 authority.
- GTO CISO / Security Program: Defines and validates baseline security requirements for public websites/domains (including DNS, vulnerability management, and incident reporting).
- Agency Director (or designee): Business owner accountable for the accuracy, integrity, and public service purpose of the agency's official websites.
- Agency Web Coordinator / Content Steward: Day-to-day owner for content publishing and site maintenance; coordinates intake requests.
- Public Information Officer (PIO): Coordinates public-facing messaging, participates in official directory verification for anti-phishing campaigns.
- Vendors/Contractors: Must comply with this Standard and State Security PSP when building, hosting, or administering state web services.

7.0 POLICY REQUIREMENTS

7.1 OFFICIAL DOMAIN STANDARDS (TARGET STATE)

The preferred standard for executive branch public websites is a verified government domain. Where feasible, agencies should use a .gov domain or an approved Nevada government namespace (for example, nv.gov and approved subdomains).

- Each public website or service must have one canonical URL published in the authoritative directory.
- Alternate URLs, legacy domains, and marketing-friendly shortcuts must redirect to the canonical URL.
- Agencies must not register or operate unofficial domains that represent Nevada state services without an approved exception or waiver (see Section 9.0).

7.2 APPROVED EXCEPTIONS (CARVE-OUTS)

- .edu domains operated by the Nevada System of Higher Education (NSHE). NSHE may opt in to coordination and directory listing.
- Legacy .state.nv.us domains may continue to operate where still required, but must be documented in the authoritative directory and have a modernization plan where feasible.
- Program-specific non-.gov domains may be approved only when required by law, grant/partner constraints, or technical limitations, and only with a waiver and compensating controls.

7.3 INTAKE PROCESS (SINGLE FRONT DOOR)

All new public websites, major platform changes, domain registrations, DNS changes affecting public access, and significant content migrations must be submitted through the statewide intake process (Service Desk / designated request form).

- Requests must identify the canonical URL, intended audience, the requested timeline, and the agency business owner.
- GTO will offer an interim, approved address under an approved Nevada government namespace when launch timelines are tight.
- Agencies should not procure a new public domain "on the side" to meet a deadline. That is how we end up with avoidable brand confusion and security risk.

7.4 BASELINE SECURITY REQUIREMENTS

Public websites and domains must comply with State Security PSP and related statewide security controls.

- Administrative access to hosting, CMS, DNS, and analytics must use multi-factor authentication (MFA).
- Sites must be covered by approved patch and vulnerability management practices.
- DNS changes must follow controlled change practices and logging requirements.
- A public security contact method should be provided (for example, a security email and/or security.txt where feasible).
- Suspected compromise or spoofing must be reported through the established incident process.

7.5 ACCESSIBILITY AND USABILITY REQUIREMENTS

Public websites must meet Nevada's Web Style Standard and accessibility expectations appropriate for government services.

- Web Style Standard (Control 4.01) applies to executive branch public internet sites within the Governor's authority.

- Web content and posted documents should be accessible (examples: proper headings, alt text, readable PDFs).
- Agencies must provide a public contact method for accessibility issues and content corrections.

7.6 CONTENT GOVERNANCE AND RECORDS

Every executive branch public website must have a documented content governance structure.

- Business owner: An agency executive accountable for the site/service.
- Content steward: Day-to-day editor lead.
- Publishing workflow: Who can publish; how changes are reviewed; how emergency updates are coordinated.
- Records retention: Website content, posted documents, and publishing records must align to retention schedules and NRS Chapter 239 requirements.

7.7 AUTHORITATIVE DIRECTORY OF OFFICIAL WEBSITES

GTO will maintain an authoritative directory of official executive branch websites and public-facing domains. This directory is intended to support public trust, incident response, and anti-phishing campaigns.

- Each agency must certify its directory entries at least quarterly (or within 10 business days of a change).
- Directory entries must include the canonical URL, agency owner, PIO contact, hosting/platform information, and exception/waiver status if applicable.
- PIOs may reference the directory for public advisories and anti-phishing messaging.

7.8 ANTI-PHISHING CONSIDERATIONS (COMMUNICATIONS ALIGNMENT)

Phishing and spoofed websites increasingly rely on lookalike domains and search advertisements to redirect victims. Agencies and PIOs should use the authoritative directory to promote simple public guidance: type known official addresses, verify .gov or approved Nevada domains, and be cautious with sponsored search results.

- Do not publish or circulate active phishing URLs in general communications; use defanged URLs and screenshots when training is required.
- When providing public guidance, emphasize domain verification (spelling + domain ending) rather than "bad grammar" cues, which are less reliable in the AI era.

8.0 PROCEDURES

8.1 NEW WEBSITE OR MAJOR CHANGE REQUEST

- Submit a request through the designated intake pathway with required details (requested URL, business owner, timeline, and content scope).

GTO reviews for domain standards, security baseline, accessibility plan, and directory entry requirements.

Assign and publish the canonical URL and required redirects.

Launch and conduct post-launch verification (redirects, HTTPS, accessibility checks, and logging).

8.2 DOMAIN/SUBDOMAIN REQUESTS

- Submit the domain request through intake with business justification and proposed naming.

GTO conducts naming review, security review (DNS controls, admin MFA, logging), and confirms directory requirements.

Implement DNS/certificates/redirects and update directory entry.

8.3 SUSPECTED SPOOFING OR LOOKALIKE DOMAINS

- Validate the official canonical URL using the authoritative directory and, when relevant, get.gov WHOIS for .gov domains.

Report suspected spoofing through the established security incident process.

Coordinate takedown/mitigation steps and consider public advisory messaging where needed (type official URLs, avoid sponsored results, verify the domain).

9.0 EXCEPTIONS AND WAIVERS

Waivers must be time-limited, documented, and approved in writing by the State CIO (or designee).

- A waiver request must include business justification, risk assessment, compensating controls, and a sunset date/transition plan.
- Approved exceptions must be listed in the authoritative directory with clear status and canonical guidance.
- If this Standard conflicts with Department of Administration directives, SAM, NAC, or NRS, the higher authority prevails.

10.0 PUBLICATION, VERSION CONTROL, AND RECORDS

This Standard will be maintained electronically and published in PDF format on the official policy repository. Replaced versions will be archived in accordance with applicable retention schedules.

This document is drafted to align with the GTO internal policy development and governance framework (plain-language drafting, version control, and retention practices).

11.0 APPROVAL

This Standard is effective upon approval by the State CIO (and any additional required sign-offs). It will be reviewed biennially or as needed based on changes in law, policy, or technology risk.

12.0 APPROVED BY

Title	Signature	Date
State CIO		4/22/2026

13.0 DOCUMENT HISTORY

Revision	Date	Change
0.1	12/20/2025	Initial draft for discussion (website/domain governance; authoritative directory; anti-phishing alignment).
0.9	12/28/2025	Expanded security and records requirements; aligned to intake and exception process.