

Information Technology Executive Council (ITEC)

ITEC 7016-P

1.0 **TITLE:** Domain Name Policy

2.0 PURPOSE: This policy establishes the mandatory use of “.ks.gov” or “.gov” domain names for all official online communications, publications, service delivery, online content design, and digital product development for covered entities within the State of Kansas.

3.0 SCOPE: This policy applies to all digital and online assets, communications, services, and content managed, developed, or utilized by entities within the State of Kansas, including official websites, web applications, email communications, online publications, and any digital products or services intended for public access or internal use by state agencies. This policy does not apply to domain names or digital assets not used for official state business or communication and not intended to represent or be associated with the State of Kansas in an official capacity. Regent institutions operating under the Kansas Board of Regents (KBOR) may continue to use their “.edu” domain names for all official online communications, publications, service delivery, online content design, and digital product development.

4.0 ORGANIZATIONS AFFECTED: This policy applies to all boards, commissions, departments, divisions, and agencies of the State of Kansas, as well as any third parties involved in processing, transmitting, or providing business capabilities on behalf of Kansas state government, hereafter referred to as Entities.

5.0 **REFERENCES:**

5.1 [DOTGOV Online Trust in Government Act of 2020 \(DOTGOV\)](#)

6.0 **DEFINITIONS:**

6.1 Alias: A second domain name that points to the first domain name. For example, an Alias for www.hello.com might be www.department.ks.gov.

6.2 Commercial Domain Name: Any domain name not maintained by the Office of Information Technology Services (OITS).

6.3 Domain Name: A unique name identifying an internet resource such as a website, consisting of alphanumeric words separated by periods.

6.4 Domain Name System (DNS): The international system for naming network resources and assigning alphanumeric names to numeric IP addresses, where domain names are registered.

- 6.5 HTTP Redirect: Occurs when a web server instructs a web browser to go to a different location for the requested web page. Redirects can be based on any part of the domain name.
- 6.6 “.gov”: A first-level internet domain name controlled by the Cybersecurity and Infrastructure Security Agency (CISA).
- 6.7 “.ks.gov”: A second-level internet domain name controlled by the Office of Information Technology Services (OITS).

7.0 **POLICY:**

This policy governs the use of “.ks.gov” or “.gov” domain names by all covered Entities. Entities may impose supplemental restrictions through their policies, provided these do not conflict with this policy.

Regent Institutions’ Domain Use

- 7.1 Regent institutions may use their “.edu” domain names for official communications, information, and services, provided they align with the security requirements, guidelines, and operational standards established by the Executive Branch Chief Information Technology Officer (CITO) or their designee(s).
- 7.2 Changes to the use of “.edu” domains by regent institutions must be reviewed and reported annually in accordance with this policy to ensure compliance with applicable security requirements.

Entities must:

Domain Name Approval and Use

- 7.3 Prioritize the use of “.ks.gov” domain names over “.gov” domain names.
- 7.4 Obtain prior approval from the OITS CTO or their designee for purchasing, activating, or using any commercial domain name. Approval from the CISA registrar is required for “.gov” domain names when applicable.
- 7.5 Ensure all domain name requests have approval from the Entity’s Chief Information Officer (CIO) or agency head. Requests must include:
 - 7.5.1 A detailed description of the domain’s intended use,
 - 7.5.2 The intended audience for the domain name,
 - 7.5.3 An explanation of why the specific domain name is needed,

- 7.5.4 A brief description of how this domain name will conform to all applicable policies and requirements, and
- 7.5.5 The name of any commercial domain name company/system being requested
- 7.6 Use government domain names (“.ks.gov” or “.gov”) for official communications, information, and services, except for third-party services operated by non-governmental entities on non-governmental domains for public interaction (e.g., social media).
- 7.7 Ensure that Entity systems hosted or operated by third parties comply with the requirements of this policy.

Reporting and Review Domains

- 7.8 Report annually all domain usage to the Chief Information Technology Architect (CITA). The report must include hostnames of internet-accessible information systems and the names of any commercial domain companies used.
- 7.9 The CITA must compile a consolidated report of all domain usage and provide it to the Chief Technology Officer (CTO) and the Chief Information Security Officer (CISO) annually for review and oversight.
- 7.10 The OITS CTO or their designee will review the use of non-“.ks.gov” and non-“.gov” domains and may require justification for continued use or direct cessation of non-compliant or inappropriate domains. Inappropriate domain names include, but are not limited to, those that are misleading, offensive, deceptive, or otherwise not reflective of the Entity’s official purpose and responsibilities.
- 7.11 In domain name conflicts or instances of inappropriate domain names, the OITS CTO or designee will work with the involved Entities to resolve issues and may deny, not renew, or transfer domain ownership to another Entity to prevent conflicts, confusion, or reputational harm. The OITS CTO or designee reserves the right to suspend or terminate domain names that do not align with the State of Kansas’s values, mission, or established guidelines.

Commercial Domain Names

- 7.12 The use of commercial domain names is discouraged and will be prohibited after January 1, 2025, unless a written exception is obtained in advance. Exceptions are issued by the Chief Information Security Officer (CISO) or their designee within Kansas Information Security Office (KISO) in consultation with the OITS CTO or their designee.

Aliases and Redirects

- 7.13 Ensure aliases that present a “.ks.gov” domain as a “.org,” “.com,” or other top-level domain will only be granted in limited circumstances with prior OITS approval.

- 7.14 Ensure redirects from “.ks.gov” must adhere to ITEC, OITS, and KISO requirements, including security, accessibility, and content standards.
- 7.15 Ensure redirects must not mask or hide the final destination, such as through URL shortening services.
- 7.16 Maintain a list of the name of the redirect, the location to which it is being redirected, and the date the redirect was made active.
 - 7.16.1 Review this list annually to ensure the continued need and functionality of redirects.
- 7.17 If a redirection occurs from a “.ks.gov” or “.gov” website to a non-“.ks.gov” or non-“.gov” website, present an exit notification or disclaimer that includes:
 - 7.17.1 The State of Kansas cannot attest to the accuracy of a non-State of Kansas site.
 - 7.17.2 Linking to a non-State of Kansas website does not constitute an endorsement by the State of Kansas or any of its employees of the sponsors of the information and products presented on the website.
 - 7.17.3 You will be subject to the destination website’s privacy policy when you follow the link.
 - 7.17.4 The State of Kansas is not responsible for Section 508 compliance (accessibility) on other websites.

Old Domain Names

- 7.18 Retain the old domain name indefinitely when transitioning to a “.ks.gov” or “.gov” domain name to prevent spoofing or misuse.
- 7.19 Monitor retained domain names for unauthorized activity.
- 7.20 Not use retained domain names unless for redirects.
- 7.21 Communicate domain name changes, transitions, or redirects to stakeholders.
- 7.22 Ensure redirects are removed once the retained domain is no longer in use.

Domain Registration and Contact Information

- 7.23 Ensure all domain names have current administrative, billing, and technical points of contact. Entities are responsible for maintaining accurate contact information.
- 7.24 Ensure all domain names are renewed before their expiration date to maintain continuous ownership and prevent unauthorized registration by third parties.

8.0 RESPONSIBILITIES:

- 8.1 Heads of Entities must establish procedures to ensure compliance with this policy.
- 8.2 The Chief Information Security Officer (CISO), Executive Branch, is responsible for maintaining this policy.

9.0 ENFORCEMENT:

- 9.1 Non-compliance with this policy may result in disciplinary action, including termination of employment for severe violations.
- 9.2 Written approval from the Kansas Information Security Office (KISO) is required for any exception to this policy.

10.0 CANCELLATION: This policy cancels and supersedes all previous versions.