Information Technology Executive Council (ITEC)

ITEC 7014-P

1.0 TITLE: Critical Vulnerability Patching Policy

2.0 PURPOSE: This policy aims to reduce the organization's exposure to cyber threats by ensuring the timely application of critical patches that address issues affecting the integrity, confidentiality, and availability of information and digital assets.

3.0 SCOPE: This policy applies to all systems and devices classified as critical infrastructure designated as external facing, serving external users or entities. This includes web servers, email servers, DNS servers, VPN endpoints, load balancers, domain controllers, telephony systems, audio-visual components, land mobile radio systems, and any other systems or services accessible from the internet. The scope includes hardware, software, associated infrastructure, and third-party services integrated into the organization's external presence, as well as internal systems that support or interact with external-facing assets.

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 NIST Special Publication 800-40 Revision 4: Guide to Enterprise Patch Management Planning

6.0 DEFINITIONS:

6.1 Critical Infrastructure: Systems essential to the operation and security of external-facing services, whose failure or compromise would impact business continuity, data security, or public safety.

6.2 Critical Issue: A serious flaw in a system or software where the only mitigation requires a critical patch to mitigate risks to security, functionality, or stability.

6.3 Critical Patch: A mandatory software update released by a vendor to address critical issues that could impact the security, functionality, or stability of a system.

6.4 Critical Vulnerability: A serious weakness in a system that, if exploited, could compromise data security or functionality.

6.5 External Facing Asset: Any system or service accessible from the internet, intended for interaction with external users or entities.

6.6 Source Vendor: The company or organization that developed the resource for which the patch was released.

6.7 Patch or Update: Software applied to fix a vulnerability or coding error.

7.0 POLICY:

This policy governs critical vulnerability patching for all State of Kansas entities. Entities may impose supplemental restrictions through their specific policies, provided these do not conflict with this policy.

Entities must:

Vulnerability Identification

7.1 Continuously monitor and scan sources such as security mailing lists, vendor notifications, KISO alerts, local security offices, and federal partners for information on critical patches for all assets within the policy scope.

Patch Procurement

7.2 Verify the source before downloading patches and obtain patches directly from the source vendor or trusted providers whenever possible.

7.3 Scrutinize and test patches from other sources carefully before introducing them into the environment to ensure their integrity and authenticity.

Patch and Update Management

7.4 Implement an accelerated patch management process to ensure the rapid application of security patches, especially for critical and high-risk vulnerabilities.

7.5 Test all patches in a controlled or limited environment before deployment.

7.6 Have a rollback plan for unsuccessful patches.

7.7 Report unsuccessful patches to the entity's change management process.

7.8 Route critical patching requests through existing change control processes.

7.9 Reboot systems as soon as practically possible as required for the patch to take effect.

Vulnerability Remediation

7.10 Apply all critical patches within twenty-four (24) hours of the vendor’s release to address critical issues.

7.11 Apply patches for high-risk vulnerabilities within five (5) days of the vendor's release for non-critical infrastructure that is not publicly available.

Compliance Monitoring and Reporting

7.12 Verify that patches have been applied successfully and that associated vulnerabilities have been mitigated.

7.13 Conduct regular audits or scans of external-facing assets to ensure compliance with this policy.

Exceptions

7.14 Document and report to Kansas Information Security Office (KISO) any deviations from this policy.

7.15 Request exceptions in writing to the KISO office. Exceptions may only be granted by the Executive Branch CISO or their designee.

7.16 Ensure all exception requests include the following:

7.16.1 Justification for the exception.

7.16.2 Assessment of the risk associated with delaying the patch or update deployment.

7.16.3 Proposed mitigation measures to reduce the risk during the delay.

7.16.4 Timeline for patch implementation.

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.