SOFTWARE SUPPLY CHAIN MANAGEMENT POLICY

Effective 11.25.25; Updated 2.14.26

1. Purpose

This policy defines how we manage and secure the software supply chain used to develop, deploy, and operate our services, including third-party libraries, frameworks, repositories, and cloud infrastructure components.

2. Scope

This policy applies to the application's source code and its associated dependencies, as well as any third-party libraries, frameworks, and plugins used in development or production. It also covers cloud-based and managed services that support the application in production, along with all software updates, patches, and configuration changes implemented throughout the system lifecycle.

3. Roles and Responsibilities

The Director of IT is responsible for overseeing software supply chain security, including approving dependencies and updates, reviewing vulnerability findings and associated remediation actions, and supervising any third-party testing or security assessments. Authorized developers and administrators are responsible for using only approved repositories and supported software versions, and for complying with all applicable change management and testing requirements.

4. Dependency and Repository Management

In alignment with secure software development lifecycle and software supply chain security controls, only currently supported operating systems, libraries, frameworks, and platforms are approved for use. Dependencies are obtained exclusively from reputable, vendor-maintained repositories to reduce supply chain risk. Deprecated or end-of-life components are routinely identified, reviewed, and replaced as part of ongoing maintenance and risk management activities. All dependency additions, updates, or removals are governed by established change management, testing, and validation procedures to ensure continued security and stability.

5. Vulnerability Management

Routine vulnerability scanning is performed using automated tools and platform-provided security services. Identified vulnerabilities are assessed for risk, prioritized based on severity and potential impact, and remediated in a timely manner for critical and high-risk findings. Periodic security assessments are also conducted to evaluate overall software and infrastructure risk and to confirm the effectiveness of security controls.

6. Testing and Change Control

All updates, patches, and dependency changes are tested prior to deployment to ensure system stability and security. Emergency changes are documented and undergo

after-the-fact review and approval. The Director of IT provides final approval for any changes that affect security controls or production systems.

7. Third-Party and Cloud Services

Cloud infrastructure is hosted on AWS and leverages AWS-provided security controls and monitoring capabilities. The use of third-party services is limited and evaluated for security and compliance impact. Vendor security documentation is reviewed as part of both initial onboarding and ongoing vendor management activities.

8. Documentation and Review

Supporting documentation, including vulnerability scan results, assessment summaries, and dependency reviews, is maintained internally. This documentation is reviewed on a periodic basis and updated as necessary to reflect current practices and risk posture. Documentation is made available upon request, subject to applicable confidentiality requirements.

9. Policy Review

This policy is reviewed at least annually and updated to reflect changes in technology, threat landscape, or regulatory expectations.