SystemSeed

Supply Chain Policy Statement

Policy Statement:

This policy outlines the requirements and standards for managing the software supply chain of SystemSeed Digital Services LLC, It aims to ensure the integrity, security, and reliability of the software development lifecycle (SDLC), from third-party component selection to deployment. Compliance with this policy is mandatory for all employees and contractors involved in software development and operations.

Scope:

This policy applies to all software development projects, including but not limited to application software, web services, and internal tools developed by SystemSeed or on its behalf.

Policy-as-Code:

SystemSeed adopts a policy-as-code (PaC) approach to automate compliance and enforcement. PaC involves using code to manage, enforce, and monitor compliance with this policy. Tools and scripts developed under this policy shall be maintained in a version-controlled repository accessible to compliance assessors.

Responsibilities:

- **Management Team:** Ensure the policy is updated in line with industry standards and regulatory requirements.
- **Project Managers:** Enforce policy compliance in their respective projects.
- **Developers:** Adhere to the policy in their development work.
- **Compliance Assessors:** Automate, monitor, and audit compliance with the policy.

1. Supplier Selection and Evaluation

- Perform due diligence on third-party suppliers of software components and services. Criteria include security practices, license compatibility, and support.
- Maintain a list of approved suppliers in a version-controlled document.

2. Component Integrity and Security

- Use automated tools to scan for vulnerabilities in third-party components.
- Enforce the use of signed packages and verify signatures before integration.
- Update components regularly to ensure security and compatibility.

3. Development and Build Process

- Implement Continuous Integration (CI) practices, ensuring that code commits trigger automated builds and tests.
- Use PaC tools to enforce coding standards and security checks during the CI process.

4. Deployment and Delivery

- Automate deployment processes to reduce human error and ensure consistent configurations.
- Use PaC tools to validate compliance with deployment standards and security policies.

5. Compliance Monitoring and Reporting

- Utilize PaC tools for continuous compliance monitoring.
- Generate compliance reports for review by the management team.

6. Incident Response and Remediation

- Establish an incident response plan for addressing security vulnerabilities and breaches.
- Automate the tracking and remediation of incidents where possible.

Signed:

Anthony Fox-Davies
CEO, SystemSeed
1st January 2024