Policy Statement

Policy Goals:

- Deliver quality systems which meet or exceed customer expectations when promised and within cost estimates
- Provide a framework for developing quality systems using an identifiable, measurable, and repeatable process
- Identify and assign the roles and responsibilities of all involved parties, including functional and technical managers, throughout the system development life cycle
- Ensure that system development requirements are well defined and subsequently satisfied.

Policy Objectives:

- Establish appropriate levels of management authority to provide timely direction, coordination, control, review and approval of the system development project
- Document requirements and maintain traceability of those requirements throughout the development and implementation process
- Ensure that projects are developed within the current and planned information technology infrastructure.

Segregation of Environments

Development will be performed in a dedicated environment, separate from quality assurance and production.

Quality Assurance will be performed in a dedicated environment separate from production and development.

System Development Life Cycle (SDLC) Phases

Initial Phase

The purposes of the Initiation Phase are to:

- Identify and validate an opportunity to improve business accomplishments or a deficiency related to a business need
- Identify significant assumptions and constraints on solutions
- Recommend the exploration of alternative concepts and methods to satisfy the need

Feasibility Phase

The Feasibility Phase is the initial investigation or brief study of the problem to determine whether the systems project should be pursued. A feasibility study establishes the context through which the project addresses the requirements and investigates the practicality of a proposed solution. The feasibility study is used to determine if the project should get the go-ahead. If the project is to proceed, the feasibility study will produce a project plan and budget estimates for the future stages of development.

Requirements Analysis Phase

This phase formally defines the detailed functional user requirements, using high-level requirements identified in the Initiation and Feasibility Phases. In this phase, the requirements are defined to a sufficient level of detail for systems design to proceed. Requirements need to be measurable, testable, and relate to the business need or opportunity identified in the Initiation Phase.

Design and Development Phase

During this phase the system is designed to satisfy the functional requirements identified in the previous phase. Since problems in the design phase can be very expensive to solve in later stages of the software development, a variety of elements are considered in the design to mitigate risk. These include:

- Identifying potential risks and defining mitigating design features
- Performing a security risk assessment
- Developing a conversion plan to migrate current data to the new system
- Determining the operating environment

Implementation, Documentation and Testing Phase

For OnCue, as part of the implementation phase, updated detailed documentation will be developed and will include all operations information including detailed instructions for when systems fail. OnCue products may not be moved into the production environment without this documented information.

Testing will be performed in its own environment and includes unit, integration, and system testing to ensure the proper implementation of the requirements.

Operations and Maintenance Phase

System operations and maintenance is ongoing. OnCue conducts an annual review with Stakeholders. The system is monitored for continued performance in accordance with user requirements and needed system modifications are incorporated when identified, approved, and tested. When modifications are identified, the system may reenter the planning phase.

Security Vulnerabilities

Managing the security vulnerabilities will be handled by the Security Team, who will identify, manage, and minimize the security vulnerabilities by code fix or configuration change (for example, by a hotfix, patch, or other way of handling the security vulnerabilities). Critical patches are assessed and evaluated within 5 business days and implemented as soon as possible. Priority certification and full QA testing is employed to validate the full system functionality and availability of the systems post-patching.

Policy Review

This policy will be reviewed at least annually by Management for effectiveness and to ensure its continued use and relevance as part of the OnCue information security management system.

Policy Enforcement

Failure to comply with this policy will result in disciplinary action up to and including termination of employment.